Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

Representation of Linear Groups as Transitive Substitution Groups.

BY LEONARD EUGENE DICKSON.

INTRODUCTION.

One of the advantages of the study of groups of congruences and of groups of linear substitutions in a general Galois field is the ability to deal with groups of high order as well as with infinite systems of groups by means of analytic formulæ involving a small number of variables. The study of finite groups defined analytically has led to such distinctive methods and the results have been given such a degree of generality that there appears to be some justification for the attitude of many specialists in the theory of substitution groups towards the analytic theory. It is hoped that the present investigation will be a first step in the direction of a closer union of these branches of group theory.

After giving in §1 a proof of the known theorem on the representation of certain quotient-groups derived from the *general* linear group as doubly transitive substitution groups, and an outline in §3 of the general method of the paper for representing the more important classes of *special* linear groups, I take up the orthogonal groups in §§4–16, the abelian linear group in §§17–20, and, finally, the hypoabelian groups in §§21–26. A similar investigation for the hyperorthogonal linear group* will form part of a paper to be presented to the Annalen. In the main, the paper is complete within itself, but occasional aid is drawn chiefly from the memoir† in which I made a study of all linear groups defined by a quadratic invariant, all of these groups being now represented as transitive substitution groups.

The group of orthogonal substitutions of determinant unity in the $GF[p^n]$ on an odd number m of variables may be represented as a transitive substitution group on $(p^{n(m-1)} - 1)/(p^n - 1)$ letters. Except for $p^n = 3$, $m \geqq 5$, this is the minimum number of letters for the methods of representation here studied. For $m = 3$, the above number is $p^n + 1$, in accord with the known[*] isomorphism of a subgroup of index 2 of the ternary orthogonal group of substitutions of determinant unity with the linear fractional group, each in the $GF[p^n]$. Aside from the cases $p^n = 5, 7, 9, 11$, the latter group cannot be represented on fewer than $p^n + 1$ letters (Moore, Wiman; and Galois, Gierster, for $n = 1$).

---

* Mathematische Annalen, vol. LII, pp. 561–581.

† American Journal, vol. XXI, pp. 193–256.

The minimum number of letters necessary for the representation (by the method under investigation) of the simple groups derived from the orthogonal group on an even number m of variables is given in §§10, 11. For the quaternary second orthogonal quotient-group $Q^{(\nu)}_{4,p^n}$, this number is $p^{2n} + 1$, in accord with the isomorphism[†] of its subgroup of index 2 with the linear fractional group in the $GF[p^{2n}]$.

These results serve on the one hand as a check and on the other hand as an indication that the method gives the minimum number of letters when p^n exceeds a certain low value.

As a special result of the investigation of the $2m$-ary hypoabelian groups (the case $n = 1$), we note that the first and second hypoabelian groups may be represented as transitive substitution groups on

$$2^{2m-1} - 2^{m-1}, \quad 2^{2m-1} - 2^{m-1} - 1$$

letters respectively (minimum values for the method here employed). This result agrees with the known isomorphism of the first hypoabelian group and the Steiner substitution group.

Finally, I would call special attention to the important property of various linear groups explained in §2.

1. A linear homogeneous substitution on m variables,

$$\mathrm{A}: \quad \xi_i' = \sum_{j=1}^{m} \alpha_{ij}\xi_j, \qquad (i = 1, 2, \ldots, m),$$

with coefficients in the Galois field of order p^n, the $GF[p^n]$, permutes amongst themselves the linear functions

$$\lambda_1\xi_1 + \lambda_2\xi_2 + \ldots + \lambda_m\xi_m, \qquad (\lambda_i \text{ in the } GF[p^n]).$$

---

[*] American Journal, l. c., p. 219.

[†] Ibid., pp. 249-255. On p. 255, F_{1,p^n}, F_{1,p_n} should read $F_{1,p^{2n}}$.

Excluding the case $\lambda_1 = \lambda_2 = \ldots\ldots = \lambda_m = 0$, these functions may be combined in sets of $p^n - 1$, those of any set being of the form

$$\mu\lambda_1\xi_1 + \mu\lambda_2\xi_2 + \ldots\ldots + \mu\lambda_m\xi_m,$$

where μ runs through the series of marks $\neq 0$ of the $GF[p^n]$. Such a set will be designated by the symbol $\{\lambda_1\xi_1 + \ldots\ldots + \lambda_m\xi_m\}$, so that there are $(p^{nm} - 1)/(p^n - 1)$ distinct symbols. A substitution A which leaves every symbol unaltered evidently has the form

$$R: \quad \xi_i' = \rho\xi_i, \qquad (i = 1, 2, \ldots\ldots, m).$$

A substitution R is commutative with every linear substitution A, so that the group of all linear substitutions A has an invariant subgroup formed of the substitutions R. The quotient-group Γ is holoedrically isomorphic with the substitution group G on the above symbols.

Moreover, G is doubly transitive. In proof, it is only necessary to show that, if two distinct symbols

$$\{\lambda_1\xi_1 + \lambda_2\xi_2 + \ldots\ldots + \lambda_m\xi_m\}, \quad \{\rho_1\xi_1 + \rho_2\xi_2 + \ldots\ldots + \rho_m\xi_m\}$$

are given, such, therefore, that the ratios $\lambda_1 : \rho_1, \ldots\ldots, \lambda_m : \rho_m$ are not all equal, there exists a linear substitution which replaces the symbols $\{\xi_1\}$ and $\{\xi_2\}$ respectively by the first and the second given symbols. If α_{ij} be chosen, as may be done, so that the determinant

$$\begin{vmatrix} \lambda_1 & \lambda_2 & \ldots\ldots & \lambda_m \\ \rho_1 & \rho_2 & \ldots\ldots & \rho_m \\ \ldots & \ldots & \ldots\ldots & \ldots \\ \alpha_{i1} & \alpha_{i2} & \ldots\ldots & \alpha_{im} \\ \ldots & \ldots & \ldots\ldots & \ldots \end{vmatrix} \neq 0,$$

the required substitution may be taken to be

$$\xi_1' = \sum_{j=1}^{m} \lambda_j\xi_i, \quad \xi_2' = \sum_{j=1}^{m} \rho_j\xi_j, \quad \xi_i' = \sum_{j=1}^{m} \alpha_{ij}\xi_j, \qquad (i = 3, \ldots\ldots, m).$$

The quotient-group Γ may be represented as a doubly transitive substitution group on $(p^{nm} - 1)/(p^n - 1)$ letters.

Of more importance than Γ is the quotient-group $LF(m, p^n)$ of the group of all linear substitutions A of determinant unity by the invariant subgroup formed of the substitutions R of determinant unity. The notation $LF(m, p^n)$ is derived from the linear fractional form in which its operators may be exhibited. Except for $p^n = 2$, $m = 2$; $p^n = 3$, $m = 3$, the group $LF(m, p^n)$ is simple.*

The above proof may be extended to the group $LF(m, p^n)$; only the ratios of the λ_i being essential, the determinant employed may be supposed equal to unity. Hence the theorem:

The linear fractional group $LF(m, p^n)$ may be represented as a doubly transitive substitution group on $(p^{nm} - 1)/(p^n - 1)$ letters.

If this method of procedure be employed in the case of a linear group possessing an invariant $\phi(\xi_1, \xi_2, \ldots, \xi_m)$, it evidently leads to an intransitive substitution group, and the number of letters is unnecessarily large. The present paper presents a general method of representing such groups as transitive permutation groups and determines which representation involves the fewest letters

2. Frequent application is made of a fundamental property possessed by various linear groups. Of the conditions upon the coefficients of the general substitution of a given linear group, let R_1 denote those involving only the coefficients of the first row of the matrix of coefficients, $R_{1,2}$ those involving only the coefficients of the first and second rows, etc. When the linear group contains a substitution in which the coefficients of the first row are *arbitrary* marks of the field which satisfy conditions R_1, a substitution in which the coefficients of the first and second rows are arbitrary marks satisfying conditions $R_{1,2}$, etc., the group will be said to possess *successive generality.*

The orthogonal, the abelian, hypoabelian and the hyperorthogonal groups possess successive generality. Certain linear groups†, the conditions upon whose coefficients are of degree > 2, do not possess this property, at least when not reduced in form [for example, if we use the conditions given by A^{-1}, §3].

3. In order that a linear substitution A shall leave formally invariant a function $\phi(\xi_1, \xi_2, \ldots, \xi_m)$, certain conditions upon the coefficients must be satisfied. Thus $\phi(\xi_1', \xi_2', \ldots, \xi_m') \equiv \phi$ requires

$$\phi(\alpha_{11}, \alpha_{21}, \ldots, \alpha_{m1}) = \phi(1, 0, \ldots, 0),$$

$$\phi(\alpha_{12}, \alpha_{22}, \alpha_{32}, \ldots, \alpha_{m2}) = \phi(0, 1, 0, \ldots, 0).$$

But conditions of this nature involve the coefficients of one or more columns of the matrix for A. To obtain the conditions involving only the coefficients of one or more rows of the matrix for A, it usually suffices to require that ϕ be invariant under A^{-1}, the inverse of the general substitution of the group. The set of conditions obtained by means of A^{-1} must of course be equivalent to the set obtained from A, but are usually in a more convenient form.

---

* Annals of Mathematics, vol. XI, pp. 161–183; University of Chicago Record, Aug., 1896.

† Quarterly Journal, July, 1899; Proc. Lond. Math. Soc., vol. XXX, p. 200.

For definiteness of expression, suppose there is a single condition $\psi(\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1m}) = c$ involving only the coefficients of the first row of the matrix of the general substitution A of the group. The substitution A replaces $\lambda_1 \xi_1 + \lambda_2 \xi_2 + \ldots + \lambda_m \xi_m$ by the function

$$\sum_{j=1}^{m} \gamma_j \xi_j, \quad \gamma_j \equiv \sum_{i=1}^{m} \alpha_{ij} \lambda_i,$$

the matrix of the coefficients of the λ^i in the γ_j being the transposed of the matrix A, viz.,

$$\begin{array}{r|cccc} & \lambda_1 & \lambda_2 & \cdots & \lambda_m \\ \hline \gamma_1 = & \alpha_{11} & \alpha_{21} & \cdots & \alpha_{m1} \\ \gamma_2 = & \alpha_{12} & \alpha_{22} & \cdots & \alpha_{m2} \\ & \cdots & \cdots & \cdots & \cdots \\ \gamma_m = & \alpha_{1m} & \alpha_{2m} & \cdots & \alpha_{mm}. \end{array}$$

Hence, if the transposed of the matrix of the general substitution of a linear group always defines a substitution of the group, the functions $\lambda_1 \xi_1 + \ldots + \lambda_m \xi_m$, where $\phi(\lambda_1, \lambda_2, \ldots, \lambda_m)$ has a constant value, are permuted amongst themselves. But this condition on the transposed matrix may not be satisfied, as, for example, when the group is the second orthogonal group in the $GF[p^n]$, $p^n = 4l + 1$ [See §4, end].

If $\lambda_1, \lambda_2, \ldots, \lambda_m$ be a set of marks, necessarily satisfying

$$(R_1) \qquad \psi(\lambda_1, \lambda_2, \ldots, \lambda_m) = c,$$

such that the group contains at least one substitution T replacing ξ_1 by $\sum_{i=1}^{m} \lambda_i \xi_i$, then the product ST belongs to the group, and hence replaces ξ_1 by a function $\Sigma \gamma_j \xi_j$ for which

$$\psi(\gamma_1, \gamma_2, \ldots, \gamma_m) = c.$$

We thus obtain a set of functions which are permuted by the group. For the groups studied in this paper, the above assumption will be satisfied for an arbitrary set of solutions $\lambda_1, \ldots, \lambda_m$ of (R_1).

The following generalization is immediate. Its statement is, however, limited to the extensive classes of linear groups possessing successive generality (§2). Employing the notations R_1, $R_{1,2}$,.. of §2, we obtain a first representation of the group as a substitution group by considering the linear functions $\lambda_1\xi_1+\lambda_2\xi_2+\dots+\lambda_m\xi_m$, where $\lambda_1, \dots, \lambda_m$ are any marks satisfying the conditions R_1; a second representation by means of a pair of linear functions $\Sigma\lambda_{1i}\,\xi_i$ and $\Sigma\lambda_{2i}\,\xi_i$, where λ_{1i}, λ_{2i} are any marks which satisfy the conditions $R_{1,2}$; a third representation by means of three linear functions with coefficients satisfying the conditions $R_{1,2,3}$; finally, a representation by means of m linear functions whose coefficients are the most general set of m^2 marks which satisfy the conditions $R_{1,2,\dots,m}$ imposed upon the general substitution of the group. Instead of the linear functions, we may, in each case, use a positional symbol, the elements of each row of which are the coefficients of the successive linear functions, thus:

$$[\lambda_1, \lambda_2, \dots, \lambda_m], \quad \begin{bmatrix}\lambda_{11}, & \lambda_{12}, & \dots, & \lambda_{1m}\\ \lambda_{21}, & \lambda_{22}, & \dots, & \lambda_{2m}\end{bmatrix}, \dots, \begin{bmatrix}\lambda_{11}, & \lambda_{12}, & \dots, & \lambda_{1m}\\ \lambda_{21}, & \lambda_{22}, & \dots, & \lambda_{2m}\\ \dots & \dots & \dots & \dots\\ \lambda_{m1}, & \lambda_{m2}, & \dots, & \lambda_{mm}\end{bmatrix}.$$

In the last case, the group is represented as a regular substitution group; indeed, the symbol represents the matrix of the general substitution of the group, so that the process, for this case, is identical with that used by Dyck.[*]

The First and Second Orthogonal Groups, §§4–16.

4. Every group of linear homogeneous substitutions on m variables with coefficients in the $GF[p^n]$, $p>2$, which is defined by a quadratic invariant of non-vanishing determinant, can be transformed by a linear homogeneous substitution belonging to the field into one of the two groups.

1°. The first orthogonal group $O^{(1)}_{m,p}$ with the invariant

$$\xi_1^2+\xi_2^2+\dots+\xi_{m-1}^2+\xi_m^2.$$

2°. The second orthogonal group $O^{(\nu)}_{m,p^n}$ with the invariant

$$\xi_1^2+\xi_2^2+\dots+\xi_{m-1}^2+\nu\xi_m^2,$$

---

[*] Mathematische Annalen, vol. XX (1882), p. 30.

where ν is a particular not-square in the $GF[p^n]$. For m odd, the second group is conjugate with the first.*

Treating together the two groups, let $O^{(\mu)}_{m,\,p^n}$ denote the orthogonal group defined by the invariant

$$\xi_1^2 + \xi_2^2 + \dots + \xi_{m-1}^2 + \mu\xi_m^2 .$$

The conditions upon the coefficients of a substitution

$$A:\ \ \xi_i' = \sum_{j=1}^{m} \alpha_{ij}\,\xi_j \qquad (i = 1, \dots, m)$$

belonging to the group are known to be the following:

$$\sum_{i=1}^{m-1} \alpha_{ij}^2 + \mu\alpha_{mj}^2 = \begin{cases} 1, & (j = 1, 2, \dots, m-1), \\ \mu, & (j = m), \end{cases} \tag{1}$$

$$\sum_{i=1}^{m-1} \alpha_{ij}\,\alpha_{ik} + \mu\alpha_{mj}\,\alpha_{mk} = 0, \quad (j, k = 1, \dots, m;\ j \neq k). \tag{2}$$

The inverse of A is, therefore,

$$A^{-1}:\ \begin{cases} \xi_i' = \displaystyle\sum_{j=1}^{m-1} \alpha_{ji}\,\xi_j + \mu\alpha_{mi}\xi_m, & (i = 1, 2, \dots, m-1). \\ \xi_m' = \dfrac{1}{\mu}\displaystyle\sum_{j=1}^{m-1} \alpha_{jm}\,\xi_j + \alpha_{mm}\,\xi_m . \end{cases}$$

Writing the relations (1) and (2) for the inverse A^{-1}, we have

$$\sum_{i=1}^{m-1} \alpha_{ji}^2 + \frac{1}{\mu}\,\alpha_{jm}^2 = \begin{cases} 1\ , & (j = 1, 2, \dots, m-1), \\ 1/\mu, & (j = m). \end{cases} \tag{1'}$$

$$\sum_{i=1}^{m-1} \alpha_{ji}\,\alpha_{ki} + \frac{1}{\mu}\,\alpha_{jm}\,\alpha_{km} = 0, \quad (j, k = 1, \dots, m;\ j \neq k). \tag{2'}$$

It follows that the transposed of the matrix of A will likewise belong to the group if, and only if, either $\mu^2 = 1$ or else

$$\alpha_{jm} = 0, \quad \alpha_{mj} = 0, \quad \alpha_{mm}^2 = 1, \quad (j = 1, 2, \dots, m-1).$$

In the latter case the substitution leaves $\xi_1^2 + \dots + \xi_{m-1}^2$ and ξ_m^2 each invariant.

---

* Dickson, American Journal, vol. XXI, pp. 193-256. This paper will be referred to as A. J., with the specific pages mentioned. Certain changes of notation, however, will be found desirable for the present use.

5. THEOREM.—*The orthogonal groups possess successive generality.*

Given a set of marks α'_{ij} of the $GF[p^n]$ such that

$$\sum_{i=1}^{m-1} \alpha'^2_{ji} + \frac{1}{\mu}\alpha'^2_{jm} = 1, \quad \sum_{i=1}^{m-1} \alpha'_{ji}\alpha'_{ki} + \frac{1}{\mu}\alpha'_{jm}\alpha'_{km} = 0, \tag{3}$$

for $j, k = 1, 2, \ldots, r, j \neq k$, where r is a given positive integer* $< m$, it is to be shown that the group $O^{(\mu)}_{m,p^n}$ contains a substitution S which replaces ξ_j by $\sum_{i=1}^{m} \alpha'_{ji}\xi_i$ for $j = 1, 2, \ldots, r$.

The theorem may be established by induction. Assuming it to be true for the case $r - 1$, it will be proved true for the case r. The theorem is true for $r = 1$ (*A. J.*, pp. 199–207; see §6 below). By the hypothesis, the group contains a substitution A' of the form A (§4) in which

$$\alpha_{ij} \equiv \alpha'_{ij} \text{ for } i = 1, 2, \ldots, r-1; j = 1, \ldots, m. \tag{4}$$

By (3), $\alpha'_{r1}, \alpha'_{r2}, \ldots, \alpha'_{rm}$ do not all vanish; moreover, the determinants of the matrix

$$\left|\begin{array}{cccc} \alpha'_{11} & \alpha'_{12} & \cdots & \alpha'_{1m} \\ \alpha'_{21} & \alpha'_{22} & \cdots & \alpha'_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha'_{r1} & \alpha'_{r2} & \cdots & \alpha'_{rm} \end{array}\right|$$

are not all zero. Hence there exists an m-ary linear substitution S_1 in the $GF[p^n]$ of non-vanishing determinant which, like the required substitution S, replaces ξ_j by $\sum_{i=1}^{m} \alpha'_{ji}\xi_i$ for $j = 1, 2, \ldots, r$. The product $A'^{-1}S_1 \equiv R$ leaves $\xi_1, \xi_2, \ldots, \xi_{r-1}$ each fixed in view of (4) and replaces ξ_r by

$$R_1\xi_1 + R_2\xi_2 + \cdots + R_m\xi_m,$$

where, for $i = 1, 2, \ldots, m-1$,

$$R_i \equiv \sum_{j=1}^{m-1} \alpha'_{rj}\alpha_{ij} + \frac{1}{\mu}\alpha'_{rm}\alpha_{im}, \quad R_m \equiv \mu\sum_{j=1}^{m-1} \alpha'_{rj}\alpha_{mj} + \alpha'_{rm}\alpha_{mm}. \tag{5}$$

In view of (3) and (4), $R_1 = R_2 = \cdots = R_{r-1} = 0$, while

$$\begin{aligned} \sum_{i=1}^{m-1} R_i^2 + \frac{1}{\mu}R_m^2 &= \sum_{j=1}^{m-1} \alpha'^2_{rj}\left\{\sum_{i=1}^{m-1} \alpha^2_{ij} + \mu\alpha^2_{mj}\right\} + \frac{1}{\mu^2}\alpha'^2_{rm}\left\{\sum_{i=1}^{m-1} \alpha^2_{im} + \mu\alpha^2_{mm}\right\} \\ &+ 2\sum_{j<k}^{1,\ldots,m-1} \alpha'_{rj}\alpha'_{rk}\left\{\sum_{i=1}^{m-1} \alpha_{ij}\alpha_{ik} + \mu\alpha_{mj}\alpha_{mk}\right\} + \frac{2}{\mu}\sum_{j=1}^{m-1} \alpha'_{rj}\alpha'_{rm}\left\{\sum_{i=1}^{m-1} \alpha_{ij}\alpha_{im} + \mu\alpha_{mj}\alpha_{mm}\right\} \\ &= \sum_{j=1}^{m-1} \alpha'^2_{rj} + \frac{1}{\mu}\alpha'^2_{rm} = 1, \end{aligned}$$

---

* For $r = m$, the theorem is true by the definition of the groups.

upon applying relations (1) and (2) and afterwards (3). Inversely, the substitution $S_1 \equiv A'R$ replaces ξ_j by the linear function $\sum_{i=1}^{m} \alpha'_{ji}\,\xi_i$ for $j = 1, 2, \ldots, r$. Hence if we construct a substitution R belonging to the orthogonal group such that R leaves fixed $\xi_1, \xi_2, \ldots, \xi_{r-1}$ and replaces ξ_r by the function

$$\sum_{i=r}^{m} R_i\,\xi_i, \quad \sum_{i=r}^{m-1} R_i^2 + \frac{1}{\mu} R_m^2 = 1,$$

the product $A'R$ may be taken as the required orthogonal substitution S.

As shown above, the quantities R_i may be defined by (5). But such a substitution R exists in the group $O^{(\mu)}_{m-r+1}$ and *à fortiori* in the group $O^{(\mu)}_{m,p^n}$ in view of the theorem above quoted (the present theorem for the case $r = 1$).

In a similar manner it may be shown that the group of orthogonal substitutions of determinant $+1$ possesses successive generality. Indeed, the theorem is true for $r = 1$, and the necessary modifications in the above proof are evident.*

6. There is a second method of proof which establishes the theorem for every r including $r = 1$. The theorem is first proved for the case $r = m - 1$ as follows. Given a set of marks

$$\alpha'_{j1}, \alpha'_{j2}, \ldots, \alpha'_{jm}, \qquad (j = 1, 2, \ldots, m-1), \quad (6,$$

satisfying relations (3) for $r = m - 1$ and therefore for $j, k = 1, 2, \ldots, m-1$; $k \neq j$, there exists a single set of marks $\alpha'_{m1}, \alpha'_{m2}, \ldots, \alpha'_{mm}$, such that the substitution

$$S:\quad \xi'_j = \sum_{i=1}^{m} \alpha'_{ji}\,\xi_i \qquad (j = 1, 2, \ldots, m)$$

has determinant unity and belongs to the group, $O^{(\mu)}_{m,p^n}$, viz.,

$$\alpha'_{m1} = (-1)^{m-1} \begin{vmatrix} \alpha'_{12} & \alpha'_{13} & \cdots & \alpha'_{1m} \\ \alpha'_{22} & \alpha'_{23} & \cdots & \alpha'_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha'_{m-12} & \alpha'_{m-13} & \cdots & \alpha'_{m-1m} \end{vmatrix}, \ldots, \alpha'_{mm} = \begin{vmatrix} \alpha'_{11} & \alpha'_{12} & \cdots & \alpha'_{1m-1} \\ \alpha'_{21} & \alpha'_{22} & \cdots & \alpha'_{2m-1} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha'_{m-11} & \alpha'_{m-12} & \cdots & \alpha'_{m-1m-1} \end{vmatrix}.$$

Since these expressions are the first minors (with proper sign prefixed) of α'_{mi} in the determinant $|\alpha'_{ji}|$, this result agrees with that giving the form of the inverse A^{-1} of the general orthogonal substitution A.

---

* In regard to the special rôle played by the index ξ_m, compare § 23.

Taking the negatives of these expressions as the values of the unknown $\alpha'_{m1}, \ldots, \alpha'_{mm}$, we obtain the unique orthogonal substitution S of determinant -1 having the prescribed coefficients (6) in the first $m-1$ rows of the matrix.

The proof of the general theorem of §5 would now proceed from the case $r = m - 1$ to the case $r = m - 2$, etc. For the first step, $\alpha'_{m-11}, \ldots, \alpha'_{m-1m}$ are to be determined so as to satisfy a quadratic relation and $m-2$ linear relations, the latter involving the (given) coefficients of the preceding $m-2$ rows of the matrix.

The method will be illustrated by the important case $m = 3$. Given any set of marks $\alpha_{11}, \alpha_{12}, \alpha_{13}$ such that

$$\alpha_{11}^2 + \alpha_{12}^2 + \frac{1}{\mu}\alpha_{13}^2 = 1, \tag{7}$$

we are to determine marks $\alpha_{21}, \alpha_{22}, \alpha_{23}$ such that

$$\alpha_{21}^2 + \alpha_{22}^2 + \frac{1}{\mu}\alpha_{23}^2 = 1, \quad \alpha_{11}\alpha_{21} + \alpha_{12}\alpha_{22} + \frac{1}{\mu}\alpha_{13}\alpha_{23} = 0. \tag{8}$$

If any $\alpha_{1i} = 0$, a solution is evident. Thus, for $\alpha_{12} = 0$, we take $\alpha_{21} = \alpha_{23} = 0$, $\alpha_{22} = 1$. If $\alpha_{11} = 0$, take $\alpha_{21} = 1$, $\alpha_{22} = \alpha_{23} = 0$. If $\alpha_{13} = 0$, take

$$\alpha_{23} = 0, \quad \alpha_{21} = -\alpha_{12}, \quad \alpha_{22} = \alpha_{11}.$$

If every $\alpha_{1i} \neq 0$, we eliminate α_{21} from (8) and obtain

$$\left(\alpha_{11}^2 + \alpha_{12}^2\right)\alpha_{22}^2 + \left(\alpha_{11}^2 + \frac{1}{\mu}\alpha_{13}^2\right)\alpha_{23}^2/\mu + \frac{2}{\mu}\alpha_{12}\alpha_{13}\alpha_{22}\alpha_{23} = \alpha_{11}^2. \tag{9}$$

If both $\alpha_{11}^2 + \alpha_{12}^2$ and $\alpha_{11}^2 + \frac{1}{\mu}\alpha_{13}^2$ vanish, the equation determines $\alpha_{22}\alpha_{23}$, so that α_{23} may be chosen as an arbitrary mark $\neq 0$, α_{21} being determined by the second condition (8). In the contrary case, we may take $\alpha_{11}^2 + \alpha_{12}^2 \neq 0$.* The equation (9) is therefore equivalent to the equation

$$\left\{\left(\alpha_{11}^2 + \alpha_{12}^2\right)\alpha_{22} + \frac{1}{\mu}\alpha_{12}\alpha_{13}\alpha_{23}\right\}^2 + \frac{1}{\mu}\alpha_{11}^2\left(\alpha_{11}^2 + \alpha_{12}^2 + \frac{1}{\mu}\alpha_{13}^2\right)\alpha_{23}^2 = \alpha_{11}^2\left(\alpha_{11}^2 + \alpha_{12}^2\right).$$

In view of (7), the coefficient of α_{23}^2 is not zero. By the theorem quoted in §9, the equation has solutions in the $GF[p^n]$,

---

* For if $\alpha_{11}^2 + \alpha_{12}^2 = 0$, $\alpha_{11}^2 + \frac{1}{\mu}\alpha_{13}^2 \neq 0$, then, by (7) μ is a square and therefore unity, so that $\alpha_{11}^2 + \alpha_{13}^2 \neq 0$ and the equations are symmetrical in α_{j1}, α_{j2}, α_{j3}.

$$\alpha_{23},\quad \left(\alpha_{11}^2 + \alpha_{12}^2\right)\alpha_{22} + \frac{1}{\mu}\,\alpha_{12}\,\alpha_{13}\,\alpha_{23},$$

and therefore solutions α_{23}, α_{22} in the field. Hence the result:*

For any set of solutions in the $GF[p^n]$, $p \neq 2$, *of equation* (7), *there exists a substitution of determinant unity in the group* $O^{(\mu)}_{3,p^n}$ *which replaces* ξ_1 *by* $\alpha_{11}\xi_1 + \alpha_{12}\xi_2 + \alpha_{13}\xi_3$.

Employing this theorem, the corresponding theorem for m variables is readily proved by induction (*A.J.* §12). We obtain therefore an independent basis for the general theorem of §5.

7. By §§ 5–6, the orthogonal group $O^{(\mu)}_{m,p^n}$ contains a substitution T which replaces ξ_1 by $\lambda_1\xi_1 + \ldots\ldots + \lambda_m\xi_m$ for any set of solutions of

$$\lambda_1^2 + \lambda_2^2 + \ldots\ldots + \lambda_{m-1}^2 + \frac{1}{\mu}\lambda_m^2 = 1. \tag{10}$$

If S be any orthogonal substitution the product ST is orthogonal and therefore replaces ξ_1 by a function $\gamma_1\xi_1 + \ldots\ldots + \gamma_m\xi_m$ for which $\gamma_1^2 + \ldots\ldots + \gamma_{m-1}^2 + \frac{1}{\mu}\gamma_m^2 = 1$. Hence S replaces $\lambda_1\xi_1 + \ldots + \lambda_m\xi_m$ by $\gamma_1\xi_1 + \ldots\ldots + \gamma_m\xi_m$. It follows that the orthogonal group may be represented as a transitive substitution group on the N functions† $\lambda_1\xi_1 + \ldots\ldots + \lambda_m\xi_m$ in which $\lambda_1, \ldots\ldots, \lambda_m$ run through every set of solutions in the $GF[p^n]$ of equation (10). The isomorphism is in fact holoedric since among the above functions occur $\xi_1, \xi_2, \ldots\ldots, \xi_{m-1}$, as well as a function involving ξ_m. But an orthogonal substitution leaving these m functions all invariant is the identity.

Similarly, the subgroup of index 2 formed of the substitutions of $O^{(\mu)}_{m,p^n}$ having determinant unity may be represented as a transitive substitution group on the above N functions.

The orthogonal group contains the substitution C changing the signs of all m variables. The group of order 2 formed by C and the identity is evidently self-conjugate under $O^{(\mu)}_{m,p^n}$. The quotient-group will be designated $Q^{(\mu)}_{m,p^n}$. Combining into a single symbol $\{\lambda_1\xi_1+\dots+\lambda_m\xi_m\}$ the pair of linear functions *

---

* Compare the intricate proof (for $n = 1$, $\mu = 1$) by Jordan, "Traité des substitutions," pp. 161–166, corrected and generalized to any n by the writer, Bull. Amer. Math. Soc., vol. 4, pp. 196–200; and to any μ, American Journal, vol. XXI, pp. 199–204. However, in the latter papers, the generators are found by the same investigation.

† The value of N is given in §9.

$$\lambda_1\xi_1+\dots+\lambda_m\xi_m,\quad -\lambda_1\xi_1-\dots-\lambda_m\xi_m,$$

we obtain a set of $\frac{1}{2}N$ letters upon which $Q^{(\mu)}_{m,p^n}$ may be represented as a transitive substitution group, if the case $m=3$, $p^n=3$ be excluded. The isomorphism of the two groups is then seen to be holoedric [§16, case (1)].

For m even, the subgroup of orthogonal substitutions of determinant unity contains the substitution C. We obtain a quotient-group which may be represented as a transitive substitution group on the above $\frac{1}{2}N$ symbols.

For m odd, the subgroup of orthogonal substitutions of determinant unity does not contain C and may therefore be represented as a transitive substitution group on the $\frac{1}{2}N$ symbols, if $p^n>3$ when $m=3$.

8. If $\lambda_1,\lambda_2,\dots,\lambda_m$ be a set of marks of the $GF[p^n]$ such that

$$\lambda_1^2+\lambda_2^2+\dots+\lambda_{m-1}^2+\frac{1}{\mu}\lambda_m^2=c, \tag{11}$$

where $c\neq 1$, there does not exist an orthogonal substitution replacing ξ_1 by $\omega\equiv\lambda_1\xi_1+\lambda_2\xi_2+\dots+\lambda_m\xi_m$, but there may exist orthogonal substitutions which replace some other function

$$\omega'\equiv\lambda_1'\xi_1+\lambda_2'\xi_2+\dots+\lambda_m'\xi_m,$$

by ω. From what follows, $\lambda_1',\dots,\lambda_m'$ must also be a set of solutions of (11). By employing a new method of procedure, we may generalize the results of §7.

As in §3, the general orthogonal substitution A replaces the function $\lambda_1\xi_1+\dots+\lambda_m\xi_m$, where $\lambda_1,\dots,\lambda_m$ satisfy (11), by

$$\sum_{j=1}^{m}\gamma_j\xi_j,\quad \gamma_j\equiv\sum_{i=1}^{m}\alpha_{ij}\lambda_i.$$

We prove that $\gamma_1,\dots,\gamma_m$ satisfy relation (11). Indeed,

$$\sum_{j=1}^{m-1}\gamma_j^2+\frac{1}{\mu}\gamma_m^2=\sum_{i=1}^{m}\lambda_i^2\left\{\sum_{j=1}^{m-1}\alpha_{ij}^2+\frac{1}{\mu}\alpha_{im}^2\right\}+2\sum_{i<k}^{1,\dots,m}\lambda_i\lambda_k\left\{\sum_{j=1}^{m-1}\alpha_{ij}\alpha_{kj}+\frac{1}{\mu}\alpha_{im}\alpha_{km}\right\}$$
$$=\sum_{i=1}^{m-1}\lambda_i^2+\frac{1}{\mu}\lambda_m^2=c,$$

---

* The proportionality factor of §1 must here be ±1 in view of (10).

upon applying (1′) and (2′) and afterwards relation (11). *Hence the totality of functions* $\lambda_1\xi_1 + \lambda_2\xi_2 + \dots + \lambda_m\xi_m$, *in which* $\lambda_1, \dots, \lambda_m$ *are solutions of* (11), *are merely permuted by an arbitrary orthogonal substitution.*

9. In evaluating N, we consider more generally the number $N^{(\mu, c)}_{m, p^n}$ of sets of solutions $\lambda_1, \lambda_2, \dots, \lambda_m$ in the $GF[p^n]$ of equation (11). This number is different according as m is even or odd, $\mu = 1$ or ν, $c = 0$, square or not-square. The value of the number is (*A. J.*, §3):

$$\begin{array}{lll} \text{For } m = 2M, & c \neq 0, & p^{n(2M-1)} \mp \varepsilon^M p^{n(M-1)}, \\ & c = 0, & p^{n(2M-1)} \pm \varepsilon^M (p^{nM} - p^{n(M-1)}). \\ \text{For } m = 2M+1, & c = 0, & p^{2nM}, \\ & c = \text{square}, & p^{2nM} \pm \varepsilon^M p^{nM}, \\ & c = \text{not-square} & p^{2nM} \mp \varepsilon^M p^{nM}, \end{array}$$

Here the upper or lower signs hold according as $\mu = 1$ or ν respectively; while ε denotes ± 1 according as $p^n = 4l \pm 1$, viz.,

$$\varepsilon \equiv (-1)^{\frac{p^n-1}{2}}$$

10. If $c \neq 0$, the sets of solutions of (11) have by pairs the same values of the ratios $\lambda_1 : \lambda_2 : \dots : \lambda_m$, viz., one set of solutions and their negatives. As in §7, we obtain a representation of $O^{(\mu)}_{m, p^n}$ upon $N^{(\mu, c)}_{m, p^n}$ letters and of $Q^{(\mu)}_{m, p^n}$ upon $\frac{1}{2} N^{(\mu, c)}_{m, p^n}$ letters (using the results of §16).

If $c = 0$, we may reduce the number of letters exactly as in §1. We discard the function given by $\lambda_1 = \lambda_2 = \dots = \lambda_m = 0$, which is invariant under every orthogonal substitution. The remaining functions may be united into groups of $p^n - 1$ each, those of one group having the same ratios $\lambda_1 : \lambda_2 : \dots : \lambda_m$. This is possible in view of the homogeneity of the orthogonal substitutions and of the relation (11) for $c = 0$. We thus obtain $(N^{(\mu, c)}_{m, p^n} - 1)/(p^n - 1)$ symbols $\{\lambda_1\xi_1 + \lambda_2\xi_2 + \dots + \lambda_m\xi_m\}$, symbols which are merely permuted upon applying an arbitrary orthogonal substitution. Since

$$N^{(\mu, 0)}_{2M, p^n} - 1 \equiv (p^{nM} \mp \varepsilon^M)(p^{n(M-1)} \pm \varepsilon^M),$$

we may state the final result, incorporating the theorems of §§12–16:

The orthogonal quotient-group $Q^{(\mu)}_{m, p^n}$, $m > 2$, *may be represented as a transitive substitution group* G *on the following number of letters:*

$$\Omega \equiv (p^{n(m-1)} - 1)/(p^n - 1), \qquad (m \textit{ odd}),$$
$$E \equiv [p^{nm/2} \mp (-1)^{m(p^n-1)/4}][p^{n(m/2-1)} \pm (-1)^{m(p^n-1)/4}] \div [p^n - 1] \quad (m \textit{ even}),$$

the upper or lower signs holding according as $\mu = 1$ or $\mu = \nu$. For m odd, the group of orthogonal substitutions of determinant unity may be represented on Ω letters.

It remains to inquire which value of c gives a representation upon the lowest number of letters.

Suppose first that m is odd ($m \geqq 3$). For $c \neq 0$,* we may choose c among the squares or not-squares so that the number of letters is the least possible (§9), viz.:

$$\omega \equiv \tfrac{1}{2}\left[p^{n(m-1)} - p^{n(m-1)/2}\right].$$

For $c = 0$, the number of letters was seen to be

$$\Omega \equiv (p^{n(m-1)} - 1)/(p^n - 1).$$

If $p^n = 3$, then $\omega < \Omega$. If $p^n \geqq 5$, the condition $\omega > \Omega$ may be written

$$(p^n - 3)\,p^{n(m-1)} - p^{n(m+1)/2} + p^{n(m-1)/2} + 2 > 0,$$

and is always satisfied since $p^{n(m-1)} \geqq p^{n(m+1)/2}$, m being $\geqq 3$.

Suppose next that m is even. The case $m = 2$ is examined in §16, the orthogonal group being then commutative; as the case $c = 0$ leads to a trivial group G, a comparison with the case $c \neq 0$ is unnecessary. Suppose then that $m \geqq 4$. The various values of $c \neq 0$ give a representation on the same number of letters (§9):

$$\omega' \equiv \tfrac{1}{2}\left[p^{n(m-1)} \mp (-1)^{m(p^n-1)/4}p^{n(m/2-1)}\right].$$

For $c = 0$, the number of letters is given by the expression E of §10. In each case the upper or lower signs are to be taken according as $\mu = 1$ or $\mu = \nu$. Consider the lowest value ω'_1 of ω' and the greatest value E_1 of E, viz.:

$$\omega'_1 \equiv \tfrac{1}{2}\left[p^{n(m-1)} - p^{n(m/2-1)}\right],\quad E_1 \equiv \left[p^{nm/2} - 1\right]\left[p^{n(m/2-1)} + 1\right] \div \left[p^n - 1\right].$$

We proceed to prove that if $p^n > 3$, $\omega'_1 > E_1$. The condition is seen to be

$$p^{n(m-1)}(p^n - 3) - 3p^{nm/2} + 3p^{n(m/2-1)} + 2 > 0.$$

Since $m \geqq 4$, $p^n \geqq 5$, we have

$$p^{n(m-1)}(p^n - 3) \geqq 2p^{n(m-1)} \geqq 10p^{n(m-2)} \geqq 10p^{nm/2}.$$

The condition is, therefore, satisfied. Hence, $\omega' > E$ if $p^n > 3$. For $p^n = 3$, the question is more delicate. Since

$$\omega' = \tfrac{1}{2}\,3^{m/2-1}\left[3^{m/2} \mp (-1)^{m/2}\right],\quad E = \tfrac{1}{2}\left[3^{m/2} \mp (-1)^{m/2}\right]\left[3^{m/2-1} \pm (-1)^{m/2}\right],$$

---

* For $p^n = 3$, $m = 3$, $c \neq 0$, the isomorphism is not holoedric (§16), so that the representation fails.

we have $\omega' > E$ or $\omega' < E$ according as $\pm\,(-1)^{m/2}$ is -1 or $+1$. Hence, for $p^n = 3$, $\omega' > E$ in the two cases $\mu = 1$ with $m/2$ odd, $\mu = \nu$ with $m/2$ even; while $\omega' < E$ when $\mu = 1$ with $m/2$ even, or $\mu = \nu$ with $m/2$ odd.

We combine our results into the theorem:

If $m > 2$, the number of letters employed in the above representation of the quotient-group $Q^{(\mu)}_{m,\,p^n}$ as a transitive substitution group is less for the case $c = 0$ than for any $c \neq 0$, except for the cases $p^n = 3$, m odd, $m > 3$; $p^n = 3$, $m/2$ even, $\mu = 1$; $p^n = 3$, $m/2$ odd, $\mu = \nu$. For the latter cases the number of letters, given by a suitably chosen mark $c \neq 0$, is*

$$\tfrac{1}{2}\left[3^{m-1} - 3^{(m-1)/2}\right] \textit{ for m odd, } m > 3; \quad \tfrac{1}{2}\left[3^{m-1} - 3^{m/2-1}\right] \textit{ for m even.}$$

12. Theorem.—*The orthogonal group $O^{(\mu)}_{m,\,p^n}$ permutes transitively the totality of symbols $\{\lambda_1\xi_1 + \lambda_2\xi_2 + \dots + \lambda_m\xi_m\}$ in which $\lambda_1, \dots, \lambda_m$ are solutions of equation* (11), *c being any fixed mark of the $GF[p^n]$.*

We are to prove that there exists an orthogonal substitution A replacing the function $\omega' \equiv \lambda_1'\xi_1 + \lambda_2'\xi_2 + \dots + \lambda_m'\xi_m$, where $\lambda_1', \dots, \lambda_m'$ form a particular set of solutions in the $GF[p^n]$, $p \neq 2$, of

$$\lambda_1'^2 + \lambda_2'^2 + \dots + \lambda_{m-1}'^2 + \frac{1}{\mu}\lambda_m'^2 = c, \tag{12}$$

by the function $\omega \equiv \lambda_1\xi_1 + \lambda_2\xi_2 + \dots + \lambda_m\xi_m$, where $\lambda_1, \dots, \lambda_m$ form an arbitrary set of solutions not all zero of the analogous relation (11).

If c is the square of a mark $\gamma \neq 0$ of the field, we may take $\lambda_1' = \gamma$, $\lambda_2' = 0, \dots, \lambda_m' = 0$. By §§5–6, there exists an orthogonal substitution A replacing ξ_1 by

$$\frac{\lambda_1}{\gamma}\xi_1 + \frac{\lambda_2}{\gamma}\xi_2 + \dots + \frac{\lambda_m}{\gamma}\xi_m,$$

$$\left(\frac{\lambda_1}{\gamma}\right)^2 + \left(\frac{\lambda_2}{\gamma}\right)^2 + \dots + \left(\frac{\lambda_{m-1}}{\gamma}\right)^2 + \frac{1}{\mu}\left(\frac{\lambda_m}{\gamma}\right)^2 = 1,$$

in view of relation (11) and $\gamma^2 = c$. Hence, A replaces $\omega' \equiv \lambda\xi_1$ by ω.

Suppose next that c is zero or a not-square. By §9, there exist in the $GF[p^n]$ more than one set of solutions of†

$$D^2 + E^2 = c \tag{13}$$

---

* For $c = 0$, the number of letters is given by the theorem of §10.

† For $m = 2$, E^2 is to be replaced by $\frac{1}{\mu}E^2$ in (13) and 1 by $\frac{1}{\mu}$ in the right member of the second equation (15). But the final equation is exactly (16).

except in the case $c=0$, -1 a not-square, when the only solution is evidently $D=E=0$. Excluding this case for the present, we proceed to determine an orthogonal substitution A which replaces $D\xi_1+E\xi_2$, where D and E satisfy (13) and $E\neq 0$, by the function ω. The conditions are evidently

$$D\alpha_{1j}+E\alpha_{2j}=\lambda_j, \qquad (j=1,\,2,\,\ldots\,,\,m \quad (14)$$

together with the conditions that A shall be orthogonal.

If α_{1j}, α_{2j} be determined so that (14) and

$$\sum_{j=1}^{m-1}\alpha_{1j}^2+\frac{1}{\mu}\,\alpha_{1m}^2=1,\quad \sum_{j=1}^{m-1}\alpha_{2j}^2+\frac{1}{\mu}\,\alpha_{2m}^2=1,\quad \sum_{j=1}^{m-1}\alpha_{1j}\alpha_{2j}+\frac{1}{\mu}\,\alpha_{1m}\alpha_{2m}=0 \qquad (15)$$

are satisfied, it follows from §5 that marks

$$\alpha_{ij} \qquad (i=3,\,\ldots\,,\,m;\ j=1,\,2,\,\ldots\,,\,m)$$

may be found such that A will be the required orthogonal substitution. Substituting the values of α_{2j} determined by (14) in the second and third relations (15), the latter become

$$D^2\left(\sum_{j=1}^{m-1}\alpha_{1j}^2+\frac{1}{\mu}\,\alpha_{1m}^2\right)-2\,D\left(\sum_{j=1}^{m-1}\alpha_{1j}\lambda_j+\frac{1}{\mu}\,\alpha_{1m}\lambda_m\right)+\sum_{j=1}^{m-1}\lambda_j^2+\frac{1}{\mu}\,\lambda_m^2=E^2,$$

$$D\left(\sum_{j=1}^{m-1}\alpha_{1j}^2+\frac{1}{\mu}\,\alpha_{1m}^2\right)-\left(\sum_{j=1}^{m-1}\alpha_{1j}\lambda_j+\frac{1}{\mu}\,\alpha_{1m}\lambda_m\right)=0.$$

In view of (11), (13) and the first relation (15), these two conditions reduce to the single condition

$$\sum_{j=1}^{m-1}\alpha_{1j}\lambda_j+\frac{1}{\mu}\,\alpha_{1m}\lambda_m=D. \qquad (16)$$

The conditions are therefore (16) and the first relation (15), say (15′). These two conditions can always be satisfied.

If $\lambda_1=\lambda_2=\ldots\ldots=\lambda_{m-1}=0$, then $\lambda_m\neq 0$ by hypothesis, so that (11) gives $\frac{1}{\mu}\,\lambda_m^2=c\neq 0$. Then (16) becomes $\frac{1}{\mu}\,\alpha_{1m}\lambda_m=D$, which determines α_{1m}. Condition (15) is the only condition upon α_{11}, α_{12}, $\ldots\ldots$, α_{1m-1}; it may be solved in the field by §9.

In the contrary case, we may take $\lambda_1\neq 0$ in view of the symmetry of (11) and (16) in λ_1, λ_2, $\ldots\ldots$, λ_{m-1}. Eliminating α_{11} between (16) and (15′), the latter may be replaced by

$$\lambda_1^2\left(\sum_{j=2}^{m-1}\alpha_{1j}^2+\frac{1}{\mu}\,\alpha_{1m}^2\right)+\left(\sum_{j=2}^{m-1}\alpha_{1j}\lambda_j+\frac{1}{\mu}\,\alpha_{1m}\lambda_m-D\right)^2=\lambda_1^2. \qquad (17)$$

If $D = 0$, then $c = E^2 \neq 0$, so that the problem, is solved as above.

For the case $m = 2$, (11) and (13) have the form

$$D^2 + \frac{1}{\mu} E^2 = c, \quad \lambda_1^2 + \frac{1}{\mu} \lambda_2^2 = c.$$

The condition (17) may be written in the successive forms

$$\frac{1}{\mu}\left(\lambda_1^2 + \frac{1}{\mu}\lambda_2^2\right)\alpha_{12}^2 - \frac{2}{\mu} D\lambda_2\alpha_{12} = \lambda_1^2 - D^2,$$

$$(c\alpha_{12} - D\lambda_2)^2 = \mu c\,(\lambda_1^2 - D^2) + D^2\lambda_2^2 = \lambda_1^2 E^2.$$

If $c = 0$, the first form of the relation determines α_{12} linearly unless $D\lambda_2 = 0$, a case evidently excluded. If $c \neq 0$, the second relation determines α_{12} in the field. Then (16) determines α_{11} in the field.

13. For $m = 3$, relation (17) may be written

$$\alpha_{12}^2\left(\lambda_1^2 + \lambda_2^2\right) + \frac{1}{\mu}\alpha_{1m}^2\left(\lambda_1^2 + \frac{1}{\mu}\lambda_m^2\right) + \frac{2}{\mu}\alpha_{12}\,\alpha_{1m}\,\lambda_2\,\lambda_m - 2D\,\alpha_{12}\,\lambda_2 - \frac{2}{\mu} D\alpha_{1m}\,\lambda_m = \lambda_1^2 - D^2. \qquad (17_3)$$

If $\lambda_1^2 + \lambda_2^2 = 0$, then $\lambda_2 \neq 0$ and the equation determines α_{12} linearly, its coefficient not vanishing for every α_{1m}. In the contrary case, we multiply (17_3) by $\lambda_1^2 + \lambda_2^2$ and obtain the equivalent equation

$$\left\{\alpha_{12}\left(\lambda_1^2 + \lambda_2^2\right) + \frac{1}{\mu}\alpha_{1m}\,\lambda_2\,\lambda_m - D\lambda_2\right\}^2 = -\frac{1}{\mu}\alpha_{1m}^2\,\lambda_1^2\,c + \frac{2}{\mu} D\alpha_{1m}\,\lambda_m\,\lambda_1^2 + \lambda_1^2\left(\lambda_1^2 + \lambda_2^2 - D^2\right).$$

If $c = 0$, then $\lambda_m \neq 0$, so that α_{1m} may be chosen to make the right member a square in the field. If $c \neq 0$, the right member may be written

$$-\frac{1}{\mu}c\lambda_1^2\left(\alpha_{1m} - Dc^{-1}\lambda_m\right)^2 + \lambda_1^2\left(\lambda_1^2 + \lambda_2^2 - D^2 + \frac{1}{\mu}D^2\lambda_m^2 c^{-1}\right).$$

Applying (11) and (13) to reduce the last term, the condition becomes

$$\left\{\alpha_{12}\left(\lambda_1^2 + \lambda_2^2\right) + \frac{1}{\mu}\alpha_{1m}\,\lambda_2\,\lambda_m - D\lambda_2\right\}^2 + \frac{1}{\mu}c\lambda_1^2\left\{\alpha_{1m} - Dc^{-1}\lambda_m\right\}^2 = c^{-1}E^2\lambda_1^2\left(\lambda_1^2 + \lambda_2^2\right).$$

This equation has solutions in the field for the two quantities in brackets (*A. J.*,

§3) and therefore (17_3) has solutions α_{12}, α_{1m}. Then (16) determines α_{11} in the field.

14. The method of procedure for $m > 3$ will be illustrated by the case $m = 4$. If $\lambda_3 = 0$, the problem reduces to the case just solved. Suppose therefore that $\lambda_3 \neq 0$. The three sums

$$\lambda_2^2 + \lambda_3^2, \quad \lambda_2^2 + \frac{1}{\mu}\lambda_m^2, \quad \lambda_3^2 + \frac{1}{\mu}\lambda_m^2$$

do not all vanish (p being $\neq 2$). If $\lambda_2^2 + \lambda_3^2 \neq 0$, we determine α_{13} from

$$\alpha_{12}\lambda_2 + \alpha_{13}\lambda_3 = 0,$$

whence (17) takes the form

$$\lambda_1^2\alpha_{12}^2\left(1 + \lambda_2^2/\lambda_3^2\right) + \frac{1}{\mu}\alpha_{1m}^2\left(\lambda_1^2 + \frac{1}{\mu}\lambda_m^2\right) - \frac{2}{\mu}D\alpha_{1m}\lambda_m = \lambda_1^2 - D^2.$$

If the coefficient of α_{1m}^2 vanishes, then $\lambda_m \neq 0$ and the equation determines α_{1m} linearly and therefore in the field. In the contrary case we complete the square in α_{1m}, when the left member becomes the sum of two squares each multiplied by marks $\neq 0$. Solutions* α_{12}, α_{1m} therefore exist in the field (*A. J.*, §3).

If $\lambda_2^2 + \frac{1}{\mu}\lambda_m^2 \neq 0$, we determine α_{1m} so that

$$\alpha_{12}\lambda_2 + \frac{1}{\mu}\alpha_{1m}\lambda_m = 0,$$

whence (17) becomes

$$\lambda_1^2\alpha_{12}^2(1 + \mu\lambda_2^2/\lambda_m^2) + \alpha_{13}^2(\lambda_1^2 + \lambda_3^2) - 2D\lambda_3\alpha_{13} = \lambda_1^2 - D^2.$$

Proceeding as before, we obtain solutions α_{12}, α_{13} in the field.

To give a treatment which shall include the case $c = 0, -1$ a not-square (not solved by the preceding method), we start with a linear function

$$\omega' \equiv D\xi_1 + E\xi_2 + F\xi_3,$$

where

$$D^2 + E^2 + \tau F^2 = c, \qquad (18)$$

$$\left(\tau = 1 \text{ for } m > 3, \quad \tau = \frac{1}{\mu} \text{ for } m = 3\right)$$

solutions of which exist (*A. J.*, §3), such that $F \neq 0$. In order that a linear substitution A shall replace ω' by $\lambda_1\xi_1 + \dots + \lambda_m\xi_m$, in which the λ_i are solutions of (11), the following conditions must be satisfied:

$$D\alpha_{1j} + E\alpha_{2j} + F\alpha_{3j} = \lambda_j, \quad (j = 1, 2, \dots, m). \qquad (19)$$

---

* If $\lambda_2^2 + \lambda_3^2 = 0$, the condition becomes $(c\alpha_{1m} - D\lambda_m)^2 = \mu E^2\lambda_1^2$ and has solutions only for $\mu =$ square. For this reason we treat the three cases in succession.

We impose also the condition that A shall be orthogonal. In view of §5, we need only consider the following orthogonal conditions:*

$$\sum_{j=1}^{m-1} \alpha_{ij}^2 + \frac{1}{\mu}\,\alpha_{im}^2 = 1 \ (i = 1,\, 2), \quad \sum_{j=1}^{m-1} \alpha_{3j}^2 + \frac{1}{\mu}\,\alpha_{3m}^2 = \begin{cases} 1 & (m > 3), \\ 1/\mu & (m = 3), \end{cases} \tag{20}$$

$$\sum_{j=1}^{m-1} \alpha_{1j}\alpha_{2j} + \frac{1}{\mu}\,\alpha_{1m}\alpha_{2m} = 0, \quad \sum \alpha_{1j}\alpha_{3j} + \frac{1}{\mu}\,\alpha_{1m}\alpha_{3m} = 0,$$
$$\sum \alpha_{2j}\alpha_{3j} + \frac{1}{\mu}\,\alpha_{2m}\alpha_{3m} = 0. \tag{21}$$

Substituting the value of α_{3j} determined by (19) in (20) and (21), we obtain the the reduced set of conditions:†

$$\sum_{j=1}^{m-1} \alpha_{1j}\lambda_j + \frac{1}{\mu}\,\alpha_{1m}\lambda_m = D, \quad \sum_{j=1}^{m-1} \alpha_{2j}\lambda_j + \frac{1}{\mu}\,\alpha_{2m}\lambda_m = E. \tag{22}$$

$$\sum_{j=1}^{m-1} \alpha_{1j}^2 + \frac{1}{\mu}\alpha_{1m}^2 = 1, \sum_{j=1}^{m-1} \alpha_{2j}^2 + \frac{1}{\mu}\,\alpha_{2m}^2 = 1, \quad \sum_{j=1}^{m-1} \alpha_{1j}\alpha_{2j} + \frac{1}{\mu}\,\alpha_{1m}\alpha_{2m} = 0. \tag{23}$$

For example, the second condition (21) becomes

$$\sum_{j=1}^{m-1} \alpha_{1j}\lambda_j + \frac{1}{\mu}\,\alpha_{1m}\lambda_m - D\Big(\sum \alpha_{1j}^2 + \frac{1}{\mu}\,\alpha_{1m}^2\Big) - E\Big(\sum \alpha_{1j}\alpha_{2j} + \frac{1}{\mu}\,\alpha_{1m}\alpha_{2m}\Big) = 0.$$

The third condition (21) takes the form

$$\begin{aligned} \Big(\sum \lambda_j^2 + \frac{1}{\mu}\,\lambda_m^2\Big) - 2D\Big(\sum \alpha_{1j}\lambda_j + \frac{1}{\mu}\,\alpha_{1m}\lambda_m\Big) - 2E\Big(\sum \alpha_{2j}\lambda_j + \alpha_{2m}\lambda_m\Big) \\ + D^2\Big(\sum \alpha_{1j}^2 + \frac{1}{\mu}\,\alpha_{1m}^2\Big) + E^2\Big(\sum \alpha_{2j}^2 + \frac{1}{\mu}\,\alpha_{2m}^2\Big) \\ + 2DE\Big(\sum \alpha_{1j}\alpha_{2j} + \frac{1}{\mu}\,\alpha_{1m}\alpha_{2m}\Big) = \tau F^2, \end{aligned}$$

where $\tau = 1$ or $1/\mu$ according as $m > 3$ or $m = 3$, the summations all extending from $j = 1, 2, \ldots, m - 1$. Upon substituting for the quantities in parentheses their values, the equation reduces to (18). If any λ_i is zero, say $\lambda_1 = 0$, we take $\alpha_{11} = \alpha_{21} = 0$ and have a similar set of equations with m replaced by $m - 1$.

---

* For $m = 3$, $\mu = \nu$, we must replace 1 by $1/\mu$ in the right member of (20) for $i = 3$, and similarly F^2 by $\frac{1}{\mu}F^2$ in (18).

† These conditions may be also obtained by requiring the inverse A^{-1} to replace $\lambda_1\xi_1 + \ldots + \lambda_m\xi_m$ by $D\xi_1 + E\xi_2 + F\xi_3$, the remaining $m - 2$ conditions being then satisfied in virtue of (19).

In proving the existence in the $GF[p_1^n]$ of a set of solutions α_{1j}, α_{2j} of equations (22) and (23), we limit the discussion, for the sake of simplicity, to the case $m=3$. Taking $\lambda_1 \neq 0$, we eliminate α_{11} and α_{21} from the three equations (23) by means of (22). We obtain equation (17_3) of §13 and a similar one with α_{12}, α_{1m}, D replaced by α_{22}, α_{2m} E respectively, and the third equation

$$\alpha_{12}\alpha_{22}(\lambda_1^2+\lambda_2^2)+\frac{1}{\mu}\alpha_{1m}\alpha_{2m}\left(\lambda_1^2+\frac{1}{\mu}\lambda_m^2\right)+\frac{1}{\mu}\lambda_2\lambda_m(\alpha_{12}\alpha_{2m}+\alpha_{22}\alpha_{1m})$$
$$-\lambda_2(D\alpha_{22}+E\alpha_{12})-\frac{1}{\mu}\lambda_m(D\alpha_{2m}+E\alpha_{1m})+DE=0. \qquad (24)$$

If $\lambda_1^2+\lambda_2^2=0$, $\lambda_1^2+\frac{1}{\mu}\lambda_m^2=0$, so that $-\frac{1}{\mu}$ is a square, we have, by addition and application of (11), $\lambda_1^2+c=0$. Hence $c\neq 0$. The three conditions may be written

$$xy=\tfrac{1}{2}(D^2-c), \quad zw=\tfrac{1}{2}(E^2-c), \quad xw+yz=DE, \qquad (25)$$

where we have set

$$x\equiv\alpha_{12}\lambda_2-D, \quad y\equiv\frac{1}{\mu}\alpha_{1m}\lambda_m-D, \quad z\equiv\alpha_{22}\lambda_2-E, \quad w\equiv\frac{1}{\mu}\alpha_{2m}\lambda_m-E.$$

Eliminating y and z from (25), we find

$$\{x(E^2-c)-DEz\}^2+z^2\frac{c}{\mu}F^2=0. \qquad (26)$$

Since $D^2-c=0$ or $E^2-c=0$ requires that c be a square, when the problem has been solved in §12, equation (26) leads to solutions z and x different from zero in the field, from which y and w are determined by (25).

If the above sums do not both vanish, their analogous rôle in the formulæ enable us to assume that $\lambda\equiv\lambda_1^2+\lambda_2^2\neq 0$. As in §13, the first and second conditions may be written in the form

$$X^2+\frac{1}{\mu}c\lambda_1^2Y^2=\lambda_1^2E\lambda c^{-1}, \quad Z^2+\frac{1}{\mu}c\lambda_1^2W^2=\lambda_1^2D\lambda c^{-1}, \qquad (27)$$

where have set

$$X\equiv\lambda\alpha_{12}+\frac{1}{\mu}\alpha_{1m}\lambda_2\lambda_m-D\lambda_2, \quad Y\equiv\alpha_{1m}-\lambda_mDc^{-1},$$
$$Z\equiv\lambda\alpha_{22}+\frac{1}{\mu}\alpha_{2m}\lambda_2\lambda_m-E\lambda_2, \quad W\equiv\alpha_{2m}-\lambda_mEc^{-1}.$$

Multiplying the third condition (24) by $\lambda\equiv\lambda_1^2+\lambda_2^2$, it may be written

$$XZ+\frac{1}{\mu}c\lambda_1^2YW=\lambda_1^2DE(\lambda_m^2c^{-1}\mu^{-1}-1)\equiv\kappa. \qquad (28)$$

For brevity, put $\rho \equiv \frac{1}{\mu} c\lambda_1^2$, $\sigma = \lambda_1^2 \lambda c^{-1}$. Then (27) and (28) give

$$\rho^2 Y^2 W^2 = (E\sigma - X^2)(D\sigma - Z^2) = (\kappa - XZ)^2.$$

From the latter equality,

$$(D\sigma X - \kappa Z)^2 + Z^2 (DE\sigma^2 - \kappa^2) = D\sigma\, (DE\sigma^2 - \kappa^2). \tag{29}$$

Applying (11), we find

$$DE\sigma^2 - \kappa^2 = \lambda^2 \lambda_1^4 c^{-2} DE\,(1 - DE).$$

In view of $\rho W^2 = D\sigma - Z^2$; equation (29) gives

$$W^2 (DE\sigma^2 - \kappa^2)\, \rho = (D\sigma X - \kappa Z)^2. \tag{30}$$

The coefficient of W^2 may, for $DE \neq 0$, be supposed to be a square, by proper choice of the particular set of solutions of (18). For each set of solutions Z, X of (29), W is determined by (30) and then Y is determined linearly by (28). The required coefficients α_{1m}, α_{2m}, α_{12}, α_{22} are then determined in the field.

15. THEOREM.—*The orthogonal group* $O_{m,\,p^n}^{(\mu)}$, $m > 2$, *is holoedrically isomorphic with the transitive substitution group on the totality of linear functions* $\lambda_1\xi_1 + \lambda_2\xi_2 + \dots + \lambda_m\xi_m$ *in which*

$$\lambda_1^2 + \lambda_2^2 + \dots + \lambda_{m-1}^2 + \frac{1}{\mu} \lambda_m^2 = c = \textit{constant}. \tag{31}$$

We prove that the identity is the only orthogonal substitution which leaves fixed all of these linear functions. In order that A leave fixed $\lambda_1\xi_1 + \dots + \lambda_m\xi_m$, it is necessary that

$$\lambda_1\alpha_{1j} + \lambda_2\alpha_{2j} + \dots + \lambda_m\alpha_{mj} = \lambda_j, \quad (j = 1, \dots, m). \tag{32}$$

If there exist m linearly independent sets of solutions of (31),

$$\lambda_{1j},\ \lambda_{2j},\ \dots,\ \lambda_{mj} \qquad (j = 1, \dots, m)$$

such, therefore, that their determinant $(\lambda_{ij}) \neq 0$, then (32) gives

$$\alpha_{1j} = \alpha_{2j} = \dots = \alpha_{jj} - 1 = \dots = \alpha_{mj} = 0, \quad (j = 1, 2, \dots, m),$$

so that A would reduce to the identity.

For the case c, a square, say σ^2, in the $GF[p^n]$, we may take the sets

$$\sigma, 0, 0, \dots, 0;\ 0, \sigma, 0, \dots, 0;\ \dots;\ 0, 0, \dots, \sigma, 0;\ \lambda_1, \lambda_2, \dots, \lambda_m,$$

where $\lambda_1, \ldots, \lambda_m$ is any set of solutions in which $\lambda_m \neq 0$. The determinant of these sets is $\sigma^{m-1}\lambda_m \neq 0$.

For c a not-square and $\mu = \nu$, a not-square, we may take as one set $0, 0, \ldots, 0, x$, where $\frac{1}{\nu} x^2 = c$, or $x^2 = \nu c =$ square. Hence, the problem is reduced to the case of $m-1$ sets of solutions of $\lambda_1^2 + \ldots + \lambda_{m-1}^2 = c$, since the determinant

$$\begin{vmatrix} \lambda_{11} & \lambda_{21} & \ldots \lambda_{m-11} & 0 \\ \lambda_{12} & \lambda_{22} & \ldots \lambda_{m-12} & 0 \\ \ldots & \ldots & \ldots & \ldots \\ \lambda_{1m-1} & \lambda_{2m-1} & \ldots \lambda_{m-1m-1} & 0 \\ 0 & 0 & \ldots 0 & x \end{vmatrix} \equiv |\lambda_{ij}| \cdot x$$

will not vanish if $m-1$ independent sets $\lambda_{1j}, \lambda_{2j}, \ldots, \lambda_{m-1j}$ exist. Hence, for $c =$ not-square, the problem reduces to the case $\mu = 1$, $m \geqq 2$,

For $m = 2$, we take the sets λ_1, λ_2 and $-\lambda_2, \lambda_1$ of determinant

$$\lambda_1^2 + \lambda_2^2 = c \neq 0.$$

For $m = 3$,* we take the three sets given by the rows of

$$\begin{vmatrix} \lambda_1 & \lambda_2 & 0 \\ -\lambda_2 & \lambda_1 & 0 \\ \lambda_1' & \lambda_2' & \lambda_3' \end{vmatrix} \equiv \lambda_3' (\lambda_1^2 + \lambda_2^2)$$

where $\lambda_1^2 + \lambda_2^2 = c$, $\lambda_1'^2 + \lambda_2'^2 + \lambda_3'^2 = c$, $\lambda_3' \neq 0$. Such solutions always exist (*A. J.*, §3). The method of procedure from the case $m = r$ to $m = r + 1$ is apparent.

There remains the case $c = 0$. Let first $m = 3$. If -1 be a square in the field, $\lambda_1^2 + \lambda_2^2 = 0$ has solutions $\lambda_1 \neq 0$. We then take

$$\begin{vmatrix} \lambda_1 & \lambda_2 & 0 \\ \lambda_2 & \lambda_1 & 0 \\ \lambda_1' & \lambda_2' & \lambda_3' \end{vmatrix} = \lambda_3' (\lambda_1^2 - \lambda_2^2) = 2\lambda_3'\lambda_1^2 \neq 0.$$

If -1 be a not-square and $\mu = \nu$, a not-square, there exist solutions in the field of $\lambda_2^2 + \frac{1}{\nu}\lambda_3^2 = 0$. Then $(\lambda_3/\nu)^2 + \frac{1}{\nu}\lambda_2^2 = 0$. We thus take

$$\begin{vmatrix} \lambda_1' & \lambda_2' & \lambda_3' \\ 0 & \lambda_2 & \lambda_3 \\ 0 & \lambda_3/\nu & \lambda_2 \end{vmatrix} \equiv 2\lambda_1'\lambda_2^2 \neq 0.$$

---

* It may be shown that it is possible to choose solutions of $\lambda_1^2 + \lambda_2^2 = c$, so that the three sets $\lambda_1, \lambda_2, 0$; $0, \lambda_1, \lambda_2$; $\lambda_2, 0, \lambda_1$ are linearly independent, i. e., such that $\lambda_1^3 + \lambda_2^3 \neq 0$.

The method employed in these two cases may be extended by induction to the case of general m.

Let next $c = 0$, $\mu = 1$, $-1 =$ not square in the $GF[p^n]$.

For $m = 3$, $\lambda_1^2 + \lambda_2^2 + \lambda_3^2 = 0$ has p^{2n} sets of solutions in the $GF[p^n]$. We prove that it is possible to choose a set $\lambda_1, \lambda_2, \lambda_3$ such that

$$\begin{vmatrix} \lambda_1 & \lambda_2 & \lambda_3 \\ \lambda_3 & \lambda_1 & \lambda_2 \\ \lambda_2 & \lambda_3 & \lambda_1 \end{vmatrix} \equiv (\lambda_1 + \lambda_2 + \lambda_3)(\lambda_1^2 + \lambda_2^2 + \lambda_3^2 - \lambda_1\lambda_2 - \lambda_1\lambda_3 - \lambda_2\lambda_3),$$

shall not vanish. Since $\lambda_1^2 + \lambda_2^2 + \lambda_3^2 = 0$, the second factor vanishes if and only if the first factor $\lambda_1 + \lambda_2 + \lambda_3$ vanishes. But if the latter vanishes then

$$\lambda_2^2 + \lambda_3^2 + \lambda_2\lambda_3 = 0$$

so that either $\lambda_2 = \lambda_3 = 0$ (which case may be excluded) or else λ_3/λ_2 is a root of $\omega^2 + \omega + 1 = 0$ in the field, where, by the symmetry of the equations, we have taken $\lambda_2 \neq 0$. In the second case,

$$\lambda_3 = \omega\lambda_2, \quad \lambda_1 = -\lambda_2 - \lambda_3 = \omega^2\lambda_2.$$

Hence, of the $p^{2n} - 1$ sets of solution not all zero, at most $2(p^n - 1)$ are to be excluded.

For $m = 4$, we obtain from the preceding sets and any fourth set λ_i' in which $\lambda_1' \neq 0$ the required independent sets:

$$\begin{vmatrix} \lambda_1' & \lambda_2' & \lambda_3' & \lambda_4' \\ 0 & \lambda_1 & \lambda_2 & \lambda_3 \\ 0 & \lambda_3 & \lambda_1 & \lambda_2 \\ 0 & \lambda_2 & \lambda_3 & \lambda_1 \end{vmatrix} \neq 0.$$

By an evident induction, m independent sets of m solutions exist.

16. It remains to study the isomorphism of the orthogonal quotient-group $Q^{(\mu)}_{m,p^n}$ with the substitution group G on the symbols $\{\lambda_1\xi_1 + \dots + \lambda_m\xi_m\}$ in which $\lambda_1, \dots, \lambda_m$ satisfy (31).

Let first $m = 2$. The case $c = 0$, $-1/\mu =$ not-square must be excluded since the only solutions are then $\lambda_1 = \lambda_m = 0$, whence G is the identity. If $-\dfrac{1}{\mu} =$ square, λ_m may be chosen arbitrarily $\neq 0$, when λ_1 has two values; the $2(p^n - 1)$ sets of solutions yield two symbols, so that G is of order 2. These results agree with those of §10 for $m = 2$, since E is then 0 or 2 according as $\pm\epsilon = -1$ or $+1$. For $m = 2$, $c \neq 0$, the number of symbols is $\frac{1}{2}(p^n \mp \epsilon)$ according as

$\mu = 1$ or ν, where $\varepsilon = (-1)^{(p^n-1)/2}$. The order of the binary orthogonal group of determinant unity is $p^n \mp \varepsilon$ and the group is commutative (*A. J.*, p. 207). Considering the self-conjugate subgroup formed by the identity and the substitution changing the signs of ξ_1 and ξ_m, the quotient-group $Q^{(\mu)}_{2,p^n}$ is a commutative group of order and degree $\frac{1}{2}(p^n \mp \varepsilon)$. By §12 it is transitive. The substitution group is therefore *regular*.* This result follows also directly from the remark at the end of §3 in connection with §6, since for $m = 2$ it is indifferent whether we employ the symbol $[\lambda_1, \lambda_2]$ or the matrix symbol.

Let next $m \geqq 3$. The holoedric isomorphism of the two groups will follow when the only substitutions leaving every symbol fixed are the identity and the substitution C, which changes the sign of every index ξ_i. Suppose therefore that A is an orthogonal substitution which leaves every symbol fixed.

Case (1): $c = \text{square} = \sigma^2$. Among the symbols occurs $\{\sigma\xi_1\}$. Then A_1 where A_1 is either A itself or else the product AC, will replace $\sigma\xi_1$ by $+\sigma\xi_1$, so that A_1 leaves ξ_1 fixed.

Among the $p^n - \varepsilon$ sets of solutions in the $GF[p^n]$ of

$$\lambda_1^2 + \lambda_2^2 = \sigma^2, \quad \varepsilon \equiv (-1)^{(p^n-1)/2},$$

occur the sets $\lambda_1 = \pm\sigma$, $\lambda_2 = 0$; $\lambda_1 = 0$, $\lambda_2 = \pm\sigma$. Hence, for $p^n > 5$, there exist solutions λ_1, λ_2 both different from zero. The corresponding symbol $\{\lambda_1\xi_1 + \lambda_2\xi_2\}$ must be unaltered by A_1. But if A_1 multiply $\lambda_1\xi_1 + \lambda_2\xi_2$ by -1 then A_1 would replace $-\lambda_1\xi_1 + \lambda_2\xi_2$ by $-3\lambda_1\xi_1 + \lambda_2\xi_2$. Since the former function leads to a symbol, so must also the latter, whence $9\lambda_1^2 + \lambda_2^2 = c$, requiring $8\lambda_1^2 = 0$ and therefore $\lambda_1 = 0$. This being impossible, A_1 must leave $\lambda_1\xi_1 + \lambda_2\xi_2$ fixed and therefore also ξ_2. Similarly, A_1 leaves fixed $\xi_3, \ldots, \xi_{m-1}$, and, if $\mu = 1$, also ξ_m, so that A_1 is the identity. If $\mu = \nu$, a not-square, there exist $p^n + \varepsilon$ sets of solutions of

$$\lambda_1^2 + \frac{1}{\mu}\lambda_m^2 = \sigma^2.$$

Excluding the sets $\lambda_1 = \pm\sigma$, $\lambda_m = 0$, there remain, if $p^n > 3$, sets with $\lambda_1 \neq 0$, $\lambda_m \neq 0$. Hence, for $p^n > 3$, A_1 leaves ξ_m fixed.

For $p^n = 5$, $\mu = \nu$, it has been shown that A_1 leaves ξ_1 and ξ_m fixed. Since there are solutions of $\lambda_i^2 + \dfrac{1}{\mu}\lambda_m^2 = \sigma^2$ with $\lambda_i \neq 0$, $\lambda_m \neq 0$, it follows that A_1 leaves ξ_i fixed. Hence, A_1 is the identity.

---

* Burnside, "The Theory of Groups," p. 177, Cor. III.

For $p^n = 5$, $\mu = 1$, we prove that A_1 leaves fixed

$$\sigma(\xi_1 + 2\xi_2 + \xi_3), \quad \sigma(\xi_1 - 2\xi_2 + \xi_3),$$

each leading to a symbol, so that A_1 leaves fixed their difference $4\sigma\xi_2$ and, therefore, ξ_2 and hence also ξ_3. In fact, if A_1 multiplies $\sigma(\xi_1 + 2\xi_2 + \xi_3)$ by -1, then A_1 replaces $\sigma(-\xi_1 + 2\xi_2 + \xi_3)$ by $\sigma(-3\xi_1 - 2\xi_2 - \xi_3)$. Since the former leads to a symbol so must the latter, whence $14\sigma^2 \equiv \sigma^2 \pmod{5}$. This being impossible, A_1 leaves fixed ξ_1, ξ_2, ξ_3, and similarly $\xi_4, \ldots, \xi_m$.

For $p^n = 3$, $\mu = -1$, a not-square, we consider the functions $\xi_1 + \xi_2 + \xi_m$ and $\xi_1 - \xi_2 + \xi_m$, each leading to a symbol, and find that A_1 must multiply each by $+1$ and hence leave ξ_2 and ξ_m fixed. Similarly, A_1 leaves $\xi_3, \ldots, \xi_{m-1}$ fixed and is the identity.

For $p^n = 3$, $\mu = 1$, the method fails, if $m = 3$, since two of the three solutions of $\lambda_1^2 + \lambda_2^2 + \lambda_3^2 = 1$ must be zero. Then A_1 is not necessarily the identity but may be the orthogonal substitution changing the signs of ξ_2 and ξ_3 and still leave every symbol unaltered.

For $p^n = 3$, $\mu = 1$, $m > 3$, A_1 must leave fixed the functions

$$\xi_1, \quad \xi_1 + \xi_2 + \xi_3 + \xi_4, \quad \xi_1 + \xi_2 + \xi_3 - \xi_4, \quad \xi_1 + \xi_2 - \xi_3 + \xi_4,$$

and hence ξ_2, ξ_3, ξ_4 and similarly every ξ_i. Indeed, if A_1 multiply $\xi_1 + \xi_2 + \xi_3 + \xi_4$ (to take an example) by -1, then A_1 replaces $-\xi_1 + \xi_2 + \xi_3 + \xi_4$ by $-3\xi_1 - \xi_2 - \xi_3 - \xi_4$, the latter not leading to a symbol.

Case (2): $c =$ not-square. There are $p^n - \varepsilon$ sets of solutions of

$$\lambda_1^2 + \lambda_2^2 = c, \quad \lambda_1 \neq 0, \quad \lambda_2 \neq 0.$$

Each set of solutions λ_1, λ_2 furnishes only one new dependent set of solutions, viz., $-\lambda_1, -\lambda_2$. Let A_1 multiply $\lambda_1\xi_1 + \lambda_2\xi_2$ by $+1$. If there be a second function $\lambda_1'\xi_1 + \lambda_2'\xi_2$ independent of the former which A_1 multiplies by $+1$, then A_1 leaves ξ_1 and ξ_2 fixed. In the contrary case, A_1 multiplies $p^n - \varepsilon - 2$ functions by -1. Among the latter, occur at least two independent functions if $p^n > 5$. Hence CA_1 leaves ξ_1 and ξ_2 fixed. Thus either A_1 or CA_1, say A_2, leaves ξ_1 and ξ_2 fixed. Then A_2 cannot multiply $\lambda_1\xi_1 + \lambda_m\xi_m$ by -1, where $\lambda_1^2 + \frac{1}{\mu}\lambda_m^2 = c$, $\lambda_1 \neq 0$, since A_2 would then replace $-\lambda_1\xi_1 + \lambda_m\xi_m$ by $-3\lambda_1\xi_1 - \lambda_m\xi_m$, whereas the latter does not define a symbol. Hence, A_2 leaves ξ_m fixed. Employing $\lambda_i\xi_i + \lambda_m\xi_m$, we see that A_2 leaves ξ_i fixed, and is, therefore, the identity.

If $p^n = 5$, and $\mu = \nu$, a not-square, the symbol $\{\lambda_m \xi_m\}$ occurs. Let A_1 denote A or AC according as the former or latter leaves ξ_m fixed. Then $\lambda_i^2 + \frac{1}{\nu}\lambda_m^2 = c$ has $p^n + \epsilon = 6$ sets of solutions and A_1 cannot multiply $\lambda_i \xi_i + \lambda_m \xi_m$ $(\lambda_i \neq 0)$ by -1. Hence, A_1 leaves every ξ_i fixed.

If $p^n = 5$, and $\mu = 1$, then 2 is a not-square, so that we may suppose that A_1 leaves $\lambda\xi_1 + \lambda\xi_2$ fixed, $2\lambda^2 = c$. Since $3(2\lambda)^2 \equiv c \pmod{5}$, the function $2\lambda(\xi_1 + \xi_2 + \xi_3)$ leads to a symbol. If A_1 multiplies it by -1, A_1 replaces $2\lambda(-\xi_1 - \xi_2 + \xi_3)$ by the excluded function $-6\lambda\xi_1 - 6\lambda\xi_2 - 2\lambda\xi_3$. Hence, must A_1 multiply the above function by $+1$ and, therefore, leave ξ_3 fixed. Employing $\lambda\xi_i + \lambda\xi_3$, we find that A_1 leaves ξ_i fixed. Hence A_1 is the identity.

If $p^n = 3$ and $\mu = \nu = -1$, we may suppose that A_1 leaves ξ_m fixed. Since $c = -1$, there exist only six sets of solutions of

$$\lambda_1^2 + \lambda_2^2 - \lambda_m^2 = -1,$$

yielding the symbols $\{\xi_1 + \xi_2\}$, $\{\xi_1 - \xi_2\}$ and $\{\xi_m\}$. Hence, if $m = 3$, A_1 need not be the identity; it may change the signs of ξ_1 and ξ_2. If, however, $m \geqq 4$, there exist functions

$$\lambda_1\xi_1 + \lambda_2\xi_2 + \lambda_3\xi_3 + \xi_m, \qquad \lambda_1^2 = \lambda_2^2 = \lambda_3^2 = 1.$$

If A_1 multiply any one of these by -1, A_1 would replace $\lambda_1\xi_1 + \lambda_2\xi_2 + \lambda_3\xi_3 - \xi_m$ by the excluded function $-\lambda_1\xi_1 - \lambda_2\xi_2 - \lambda_3\xi_3$. Hence, the multiplier is always $+1$, so that A_1 is the identity.

Case (3): $c = 0$, $-1 = i^2$, i a mark of the $GF[p^n]$. Among the symbols occur $\{\xi_1 \pm i\xi_2\}$. If A multiply $\xi_1 + i\xi_2$ by ρ and $\xi_1 - i\xi_2$ by σ, then A replaces ξ_1 and ξ_2 by the respective functions

$$\tfrac{1}{2}(\rho + \sigma)\xi_1 + \frac{i}{2}(\rho - \sigma)\xi_2, \quad -\frac{i}{2}(\rho - \sigma)\xi_1 + \tfrac{1}{2}(\rho + \sigma)\xi_2.$$

By the orthogonal conditions $\rho\sigma = 1$ while ξ_j $(j > 2)$ is replaced by a function not involving ξ_1 or ξ_2. If $m = 3$, ξ_m is replaced by $\pm\xi_m$. If $m > 3$, we consider the symbols $\{\xi_1 \pm i\xi_j\}$ for $j = 3, \ldots, m - 1$ and find that ξ_1 is replaced by a function of ξ_1 and ξ_j. Combining this with the earlier result, ξ_1 is replaced by a function of ξ_1 only and $\rho = \sigma = \pm 1$. If $m > 3$, it follows that A is the identity or C. For $m = 3$, $\mu = 1$, the same result evidently holds. Finally, for $m = 3$, $\mu = \nu$, there exist sets of solutions of

$$\lambda_1^2 + \lambda_2^2 + \frac{1}{\nu}\lambda_m^2 = 0, \qquad (\lambda_1 \neq 0). \qquad (33)$$

Let A replace $\lambda_1\xi_1+\lambda_2\xi_2+\lambda_m\xi_m$ by κ and $-\lambda_1\xi_1-\lambda_2\xi_2+\lambda_m\xi_m$ by λ. Then A replaces $2\lambda_m\xi_m$ by $(\kappa-\lambda)\,\lambda_1\xi_1+(\kappa-\lambda)\,\lambda_2\xi_2+(\kappa+\lambda)\,\lambda_m\xi_m$. But, for $m=3$, A was shown to replace ξ_m by $\pm\,\xi_m$. Hence $\kappa=\lambda=\pm 1$, so that A multiplies $\lambda_1\xi_1+\lambda_2\xi_2$ by $\pm\,1$. Similarly, A multiplies $\lambda_1\xi_1-\lambda_2\xi_2$ by $\pm\,1$. Hence, A is either the identity or C.

Case (4): $c=0$, $-1=$ not-square. If $\mu=\nu$, we may take $\mu=-1$ and consider the symbols $\{\xi_1\pm\xi_m\}$, $\{\xi_m\pm\xi_j\}$ for $j=2,\ldots,m-1$, when, as in Case (3), A is seen to be the identity or C.

If, however, $\mu=1$, there exist no symbols involving only one or two indices. Consider the $p^{2n}-1$ sets of solutions of

$$\lambda_1^2+\lambda_2^2+\lambda_3^2=0, \qquad (\lambda_1\neq 0). \qquad (33')$$

Each set furnishes exactly p^n-1 dependent sets obtained by multiplying the given set by the various marks $\neq 0$ of the $GF[p^n]$. Hence, there are p^n+1 groups of dependent sets, those of different groups being independent sets. Hence, there are at least two independent sets

$$(\lambda) \qquad \lambda_{11},\ \lambda_{12},\ \lambda_{13};\ \lambda_{21},\ \lambda_{22},\ \lambda_{23}, \qquad (\text{not every } \lambda_{2j}=\sigma\lambda_{1j})$$

leading to linear functions which A multiplies by the same factor ρ. If the quantities

$$\alpha\lambda_{11}+\beta\lambda_{21}, \quad \alpha\lambda_{12}+\beta\lambda_{22}, \quad \alpha\lambda_{13}+\beta\lambda_{23}$$

be solutions of (33′), then $2\alpha\beta\tau=0$, $\tau\equiv\lambda_{11}\lambda_{21}+\lambda_{12}\lambda_{22}+\lambda_{13}\lambda_{23}$. If $\tau=0$, every one of these sets of quantities would be a solution of (33′), so that every linear function $\lambda_1\xi_1+\lambda_2\xi_2+\lambda_3\xi_3$ would be multiplied by ρ. Then would A multiply each index by ρ, so that $\rho^2=1$, requiring that S be the identity or C [proof as in §15, the right member of (32) being $\rho\lambda_j$]. If, however, $\tau\neq 0$, either $\alpha=0$ or $\beta=0$, so that only $2(p^n-1)$ of the sets of solutions of (33′) are derived linearly from the sets (λ). There remain $(p^n-1)^2$ sets linearly independent of the sets (λ). If any one of these leads to a linear function $\lambda_1\xi_1+\lambda_2\xi_2+\lambda_3\xi_3$ which A multiplies by ρ, then A multiplies ξ_1, ξ_2 and ξ_3 by $\rho=\pm\,1$ (§15). In the contrary case, they lead to at least two independent functions which A multiplies by the same constant κ, since they may be separated into p^n-1 independent groups of sets, none of which lead to a multiplier ρ. Eliminating ξ_3, we obtain a function $a_1\xi_1+a_2\xi_2$ which A multiplies by κ. Likewise from the sets (λ) we obtain a function $b_1\xi_1+b_2\xi_2$ which A multiplies by κ. Since $\kappa\neq\rho$, these functions are independent, so that A replaces ξ_1 and ξ_2 by functions of ξ_1 and ξ_2 only. If $m=3$, A replaces ξ_3 by $\pm\xi_3$ in view of the orthogonal conditions, so that A multiplies the functions derived from (λ) by ρ and, therefore, multiplies ξ_1 and ξ_2 each by ρ. If $m>3$, we make the above argument with ξ_2 replaced by ξ_i ($i=4, \ldots\ldots, m$) and see that ξ_1, and then every ξ_j, is multiplied by a contant.

We may combine our results into the theorem:

The orthogonal quotient-group $Q^{(\mu)}_{m, p^n}$, $m>2$, *is holoedrically isomorphic with he corresponding substitution group on the symbols* $\{\lambda_1\xi_1, + \ldots\ldots + \lambda_m\xi_m\}$ *in which* $\lambda_1^2 + \ldots\ldots + \lambda_{m-1}^2 + \dfrac{1}{\mu}\lambda_m^2$ *is a constant* c, *the cases* $m=3$, $p^n=3$, $\mu=1$ *or* ν *begin exceptional if* $c \neq 0$.

For the simple groups defined by the orthogonal groups* and the corresponding substitution groups, the isomorphism must, of course, be holoedric. By a study of all the invariant subgroups of $Q^{(\mu)}_{m, p^n}$, the above theorem may be otherwise established. For the exceptional case $p^n=3$, $m=3$, the orthogonal groups are of special structure, being then solvable groups.

The abelian linear group, §§17–20.

17. For the substitutions of the abelian group we employ the notation

$$\xi_i' = \sum_{j=1}^{m} (\alpha_{ij}\xi_j + \gamma_{ij}\eta_j), \quad \eta_i' = \sum_{j=1}^{m} (\beta_{ij}\xi_j + \delta_{ij}\eta_j), \qquad (34)$$
$$(i = 1, 2, \ldots\ldots m),$$

the number of indices 2^m being even.

The general abelian group† G is composed of all the substitutions (34) with coefficients in the $GF\,[p^n]$ satisfying the conditions

$$\sum_{j=1}^{m} (\alpha_{ij}\delta_{ij} - \gamma_{ij}\beta_{ij}) = \mu, \quad \sum_{j=1}^{m} (\alpha_{ij}\delta_{kj} - \gamma_{ij}\beta_{kj}) = 0, \qquad (35)$$

$$\sum_{j=1}^{m} (\alpha_{ij}\gamma_{kj} - \gamma_{ij}\alpha_{kj}) = 0, \quad \sum_{j=1}^{m} (\beta_{ij}\delta_{kj} - \delta_{ij}\beta_{kj}) = 0, \qquad (36)$$
$$(i, k = 1, \ldots\ldots, m;\ i \neq k),$$

since they must leave invariant, up to a factor $\mu \neq 0$, the function

$$\phi \equiv \sum_{i=1}^{m} (x_i Y_i = y_i X_i),$$

---

* American Journal, vol. XXI.

† Dickson, Quarterly Journal, 1897, pp. 169-178. It will be refered to as Q. J.

when operating simultaneously upon the two sets of indices

$$x_i,\ y_i;\quad X_i,\ Y_i. \qquad (i=1,\ldots,m)$$

If $\mu = 1$, so that ϕ is an absolute invariant, a subgroup H is defined, which is called the special abelian group.

For $m > 1$, the maximal invariant subgroup of H is composed of the identity and the substitution changing the signs of all $2m$ indices, the case $m=2$, $p^n = 2$ being an exception, H being then isomorphic with the symmetric group on 6 letters. The quotient group will be designated $A\ (2m, p^n)$. It is *simple* except for $m=1$, $p^n=2$; $m=1$, $p^n=3$; $m=2$, $p^n=2$.

18. THEOREM.—*The special abelian group possesses successive generality.*

The relations (35) and (36) do not explicitly include a relation involving only the coefficients α_{1j}, γ_{1j} of the first row of the matrix for (34), but the first relation (35) requires (since $\mu \neq 0$) that the coefficients α_{1j}, γ_{1j} shall not all vanish. But for α_{1j}, γ_{1j} arbitrary marks not all zero, H contains (*Q. J.*, p. 171) a substitution replacing ξ_1 by

$$\omega \equiv \sum_{j=1}^{m} (\alpha_{1j}\xi_j + \gamma_{1j}\eta_j).$$

To prove the theorem for the next step, let α_{1j}, γ_{1j}, β_{1j}, δ_{1j} be an arbitrary set of marks of the $GF[p^n]$ such that

$$\sum_{j=1}^{m} (\alpha_{1j}\delta_{1j} - \gamma_{1j}\beta_{1j}) = 1. \qquad (37)$$

We are to prove that H contains a substitution S which replaces ξ_1 by ω and η_1 by the function

$$\omega_1 \equiv \sum_{j=1}^{m} (\beta_{1j}\xi_j + \delta_{1j}\eta_j).$$

By the case already considered, H contains a substitution

$$A:\quad \xi_i' = \sum_{j=1}^{m} (\alpha_{ij}'\xi_j + \gamma_{ij}'\eta_j),\quad \eta_i' = \sum_{j=1}^{m} (\beta_{ij}'\xi_j + \delta_{ij}'\eta_j), \qquad (i=1,\ldots,m)$$

in which $\alpha_{1j}' \equiv \alpha_{1j}$, $\gamma_{1j}' \equiv \gamma_{1j}$, the coefficients subject to relations (35) and (36), when $\mu = 1$ and the letters are primed. The inverse of A is

$$A^{-1}:\quad \xi_i' = \sum_{j=1}^{m} (\delta_{ji}'\xi_j - \gamma_{ji}'\eta_j),\quad \eta_i' = \sum_{j=1}^{m} (-\beta_{ji}'\xi_j + \alpha_{ji}'\eta_j). \qquad (i=1,\ldots,m)$$

Since the ratios $\beta_{1j} : \alpha_{1j}$, $\delta_{1j} : \gamma_{1j}$ are not all equal in virtue of (37), there exists a substitution S_1, with coefficients in the $GF\,[p^n]$ of determinant not zero, which replaces ξ_1 by ω and η_1 by ω_1. Hence the product $A^{-1} S_1 \equiv R$ leaves ξ_1 fixed and replaces η_1 by

$$\rho \equiv \sum_{j=1}^{m} (\rho_j \xi_j + r_j \eta_j),$$

$$\rho_j \equiv \sum_{i=1}^{m} (\beta_{1i} \delta'_{ji} - \delta_{1i} \beta'_{ji}), \quad r_j \equiv \sum_{i=1}^{m} (-\beta_{1i} \gamma'_{ji} + \delta_{1i} \alpha'_{ji}), \qquad (j = 1, \ldots, m).$$

In particular $r_1 = 1$ by (37) since $\alpha'_{1i} = \alpha_{1i}$, $\gamma'_{1i} = \gamma_{1i}$. Since $S_1 = AR$, the product AR replaces ξ_1 by ω and η_1 by ω_1. The required abelian substitution S may therefore be taken to be AR', if there exist in H a substitution R' which, like R, replaces ξ_1 by ξ_1 and η_1 by ρ. Such a choice of R' is possible since (*Q. J.* p. 172) the group H contains a substitution leaving ξ_1 fixed and replacing η_1 by $\sum_{j=1}^{m} (\rho_j \xi_j + r_j \eta_j)$, where $r_1 = 1$ and the remaining ρ_j, η_j are any marks.

The general case of the theorem may be established by induction (compare §5), the method of proof being quite similar to that just employed in proving the first cases of the theorem.

COROLLARY. *The general abelian group G possesses successive generality.*

The substitution of H which replaces ξ_1 by ω, for α_{1j}, γ_{1j} arbitrary marks not all zero, belongs to the larger group G. To prove the next case of the theorem, in which α_{1j}, γ_{1j} β_{1j}, δ_{1j} are any marks satisfying the first condition (35) for $i = 1$, we need only take as the required substitution replacing ξ_1 by ω and η_1 by ω_1 the product ST where S is the substitution of H (determined as above) which replaces ξ_1 by ω and η_1 by $\frac{1}{\mu}\,\omega_1$ and T is the substitution of G which alters only η_1, multiplying it by μ.

19. An abelian substitution (34) replaces the linear function

$$z \equiv \sum_{i=1}^{m} (x_i \xi_i + y_i \eta_i) \tag{38}$$

by the function $z' \equiv \sum_{i=1}^{m} (x'_i \xi_i + y'_i \eta_i)$, where

$$x'_i \equiv \sum_{j=1}^{m} (\alpha_{ji} x_j + \beta_{ji} y_j), \quad y'_i \equiv \sum_{j=1}^{m} (\gamma_{ji} x_j + \delta_{ji} y_i), \tag{39}$$
$$(i = 1, \ldots, m),$$

Expressed in the matrix notation, these relations become

$$\begin{array}{r|ccccccc} & x_1 & y_1 & x_2 & y_2 & & x_m & y_m \\ \hline x_1' = & \alpha_{11} & \beta_{11} & \alpha_{21} & \beta_{21} & \cdots\cdots & \alpha_{m1} & \beta_{m1} \\ y_1' = & \gamma_{11} & \delta_{11} & \gamma_{21} & \delta_{21} & \cdots\cdots & \gamma_{m1} & \delta_{m1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ x_m' = & \alpha_{1m} & \beta_{1m} & \alpha_{2m} & \beta_{2m} & \cdots\cdots & \alpha_{mm} & \beta_{mm} \\ y_m' = & \gamma_{1m} & \delta_{1m} & \gamma_{2m} & \delta_{2m} & \cdots\cdots & \gamma_{mm} & \delta_{mm} \end{array}$$

the matrix being thus the transposed of the matrix of substitution (34). But if (34) be abelian, then is also the substitution given by the transposed of its matrix. In fact, the conditions that the latter be abelian are precisely the conditions that the inverse of (34) shall be abelian (Q. J., p. 170).

As a first result, we observe that the $p^{2nm}-1$ functions z, obtained by allowing $x_1, \ldots\ldots, x_m, y_1, \ldots\ldots, y_m$ to run through every set of $2m$ marks not all zero of the $GF[p^n]$, are permuted transitively* by an arbitrary abelian substitution (34). Combining into a single symbol $\{z\}$ the functions κz, where κ runs through the series of marks $\neq 0$ of the $GF[p^n]$, we obtain a set of $(p^{2nm}-1)/(p^n-1)$ symbols which are permuted transitively by an arbitrary abelian substitution. This result corresponds to that of §1 for the general linear group on $2m$ indices. The substitution group is, however, not doubly transitive in the case of the abelian group (see the next paragraph).

The abelian quotient-group $A(2m, p^n)$ *may be represented*† *as a simply transitive substitution group on* $(p^{2nm}-1)/(p^n-1)$ *letters.*

To obtain other (less immediate) results, we consider in connection with (39) a second set of functions

$$Z \equiv \sum_{i=1}^{m} (X_i\xi_i + Y_i\eta_i).$$

Upon applying (34), Z is replaced by $Z' \equiv \Sigma\,(X_i'\xi_i + Y_i'\eta_i)$, where X_i' and Y_i' are expressed in terms of X_i, Y_i by formulas similar to (39), i. e., by means of a matrix which is the transposed of the matrix of substitution (34). It follows that, if (34) be abelian, the following function is an invariant: *

---

* The relations (39) may be solved for x_j, y_j $(j=1, \ldots\ldots, m)$ since the determinant of their coefficients is not zero, being equal to the determinant of (34).

† A special abelian substitution leaving every symbol $\{z\}$ fixed, is either the identity or changes the signs all the indices.

$$\sum_{i=1}^{m} (x_i' Y_i' - y_i' X_i') = \sum_{i=1}^{m} (x_i Y_i - y_i X_i).$$

Introducing a positional symbol as in §3, we may state our result in the form:

An abelian substitution permutes amongst themselves the totality of symbols

$$\begin{bmatrix} x_1 & y_1 & x_2 & y_2 & \dots\dots & x_m & y_m \\ X_1 & Y_1 & X_2 & Y_2 & \dots\dots & X_m & Y_m \end{bmatrix}, \quad \sum_{i=1}^{m} (x_i Y_i - y_i X_i) = c,$$

in which c is any constant mark of the $GF[p^n]$.

For the case $c = 1$, the above symbols include the following:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \dots\dots & 0 & 0 \\ 0 & 1 & 0 & 0 & \dots\dots & 0 & 0 \end{bmatrix}.$$

Hence, by §18, *the totality of symbols given by $c = 1$ are permuted transitively by the special abelian group H and, à fortiori, by the general abelian group G.*

More generally, let c be any mark $\neq 0$. By §18, H contains a substitution S replacing ξ_1 and η_1 by the respective functions

$$\sum_{i=1}^{m} (x_i \xi_i + y_i \eta_i), \quad \sum_{i=1}^{m} (X_i c^{-1} \xi_i + Y_i c^{-1} \eta_i),$$

since, by hypothesis,

$$\sum_{i=1}^{m} (x_i Y_i c^{-1} - y_i X_i c^{-1}) \equiv c^{1-} \sum_{i=1}^{m} (x_i Y_i - y_i X_i) = c^{-1} c = 1.$$

Hence, S replaces the first by the second of the following symbols:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \dots\dots & 0 & 0 \\ 0 & c & 0 & 0 & \dots\dots & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} x_1 & y_1 & x_2 & y_2 & \dots\dots & x_m & y_m \\ X_1 & Y_1 & X_2 & Y_2 & \dots\dots & X_m & Y_m \end{bmatrix}.$$

The totality of symbols defined by a given mark $c \neq 0$ are permuted transitively by the special abelian group.

There remains the case $c = 0$. The case $m = 1$ may be excluded as trivial. In fact, X_1, Y_1 are then proportional to x_1, y_1 (not both of which are zero), so that the function Z is a constant ($\neq 0$) times the function z, and, therefore, the employment of a symbol of two rows has no advantage over the use of a symbol of one row, a case previously studied. Indeed, for $m = 1$, the abelian group is the general binary linear group.

---

* While the result is derived by means of ϕ of §17, the two invariants are not to be confused, the one formed of variables and the other of coefficients.

Suppose that $m > 1$. In the applications to be made, a symbol is to be excluded as trivial when $X_i = \rho x_i$, $Y_i = \rho x_i$ $(i = 1, \ldots, m)$. A linear substitution evidently replaces a trivial symbol by a trivial symbol and a non-trivial symbol by a non-trivial one. Consider the following special and general symbols given by $c = 0$:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \ldots\ldots 0 & 0 \\ 0 & 0 & 1 & 0 \ldots\ldots 0 & 0 \end{bmatrix}; \quad \begin{bmatrix} x_1 & y_1 & \ldots\ldots x_m & y_m \\ X_1 & Y_1 & \ldots\ldots X_m & Y_m \end{bmatrix}, \quad \sum_{i=1}^{m} (x_i Y_i - y_i X_i) = 0,$$

of which the first is not trivial and the second is assumed to be not trivial. In order that a linear substitution (34) shall replace the former by the latter symbol, following conditions are necessary and sufficient:

$$\alpha_{1i} = x_i, \quad \gamma_{1i} = y_i, \quad \alpha_{2i} = X_i, \quad \gamma_{2i} = Y_i, \quad (i = 1, 2, \ldots, m).$$

Hence the first and third rows of the matrix of (34) are determined, and, indeed, so that the abelian condition involving them [formula (36) for $i = 1$, $k = 2$] is satisfied. To determine the coefficients of the remaining rows so that (34) shall be a special abelian substitution, it suffices, in view of the theorem of §18, to determine β_{1i}, δ_{1i} $(i = 1, \ldots, m)$ of the second row, so that

$$\sum_{i=1}^{m} (\delta_{1i} x_i - \beta_{1i} y_i) = 1, \quad \sum_{i=1}^{m} (\delta_{1i} X_i - \beta_{1i} Y_i) = 0.$$

For $m \gtreqless 2$, these two equations may always be solved in the field. Suppose that $X_1 \neq 0$, changing if necessary the notation. The second relation then determines δ_{11}. Substituting this value in the first, we obtain the equivalent condition

$$\sum_{i=2}^{m} \delta_{1i} (x_i X_1 - X_i x_1) - \sum_{i=1}^{m} \beta_{1i} (y_i X_1 - Y_i x_1) = X_1.$$

This relation for $\delta_{12}, \ldots, \delta_{1m}, \beta_{11}, \beta_{12} \ldots, \beta_{1m}$ may always be solved (with, in fact, $2m - 2$ of them arbitrary) unless the coefficients on the left all vanish. But this would require that the ratios x_i / X_i, y_i / Y_i $(i = 1, \ldots, m)$ should all be equal, since equal to x_1 / X_1, which is contrary to hypothesis. We have the result:

The non-trivial symbols given by $c = 0$ are permuted transitively by the special abelian group.

20. The number of sets of solutions in the $GF[p^n]$ of

$$\sum_{i=1}^{m} (x_i Y_i - y_i X_i) = c \tag{40}$$

is $p^{n(2m-1)}(p^{2mn} - 1)$ or $p^{n(2m-1)}(p^{2mn} - 1 + p^n)$ according as $c \neq 0$ or $c = 0$. For $c = 1$ this result follows from §18 in connection with Q. J., §§6–7. But the same number of solutions exists for any $c \neq 0$ as for $c = 1$. Indeed, if x_i', y_i', X_i', Y_i' be a set of solutions when $c = 1$, then x_i', y_i', cX_i', cY_i' gives a set of solutions of (40); two sets of the latter type are identical only when the two corresponding sets of the former type are the same. Subtracting $p^n - 1$ times the number of sets when $c = 1$ from p^{4mn}, the total number of sets of $4m$ marks, we obtain the number of sets for $c = 0$.

Of the solutions of (40) when $c = 0$, the following are to be excluded: the p^{2mn} sets in which $x_i = y_i = 0$ while X_i, Y_i are arbitrary; the $p^n(p^{2mn} - 1)$ sets in which x_i, y_i are not all zero, while $X_i = \rho x_i$, $Y_i = \rho y_i$ $(i = 1, \ldots, m)$, giving the trivial symbols. There remain

$$(p^{2mn} - 1)(p^{n(2m-1)} - p^n).$$

For $m = 1$, this number vanishes, agreeing with the result in §19.

Combine into a single new symbol $\{\;\}$ all the symbols $[\;]$ which are derived by multiplication as follows:

$$\begin{Bmatrix} x_1 & y_1 & \cdots & x_m & y_m \\ X_1 & Y_1 & \cdots & X_m & Y_m \end{Bmatrix} \equiv \begin{bmatrix} \mu x_1 & \mu y_1 & \cdots & \mu x_m & \mu y_m \\ \nu X_1 & \nu Y_1 & \cdots & \nu X_m & \nu Y_m \end{bmatrix}.$$

If $c \neq 0$, then by (40) $\mu\nu = 1$, so that the symbols are combined in sets of $p^n - 1$. If $c = 0$, they are combined in sets of $(p^n - 1)^2$. We obtain the following numbers of new symbols:

$$p^{n(2m-1)}(p^{2mn} - 1)/(p^n - 1) \text{ for } c \neq 0;$$
$$(p^{2mn} - 1)(p^{n(2m-1)} - p^n)/(p^n - 1)^2 \text{ for } c = 0.$$

The latter number is less than the former. Each is greater than the number of letters required by the method, explained at the beginning of §19, except for the excluded case $m = 1$.

Whether or not the employment of symbols involving three or more rows would lead to a representation on a fewer number of letters is not evident. Such an investigation would naturally proceed upon lines similar to those used above.

The first and second hypoabelian groups, §§21–26.

21. Every group of linear homogeneous substitutions on M variables with coefficients in the $GF\,[2^n]$, which is defined by a quadratic invariant not expressible in the field as a quadratic function of fewer than M variables, is holoedrically isomorphic with one of the three groups (A. J., pp. 222–224, pp. 243–246): the first hypoabelian group G_0, the second hypoabelian group $G_{\lambda'}$, each on $M \equiv 2m$ indices, the special abelian group in the $GF\,[2^n]$ on $M - 1 \equiv 2m$ indices.

To complete the investigation of the representation of linear groups defined by a quadratic invariant, there remains the case of the hypoabelian groups G_λ, composed of all substitutions (34) in the $GF\,[2^n]$ which leave formally invariant

$$F_\lambda \equiv \sum_{i=1}^{m} \xi_i \eta_i + \lambda \xi_1^2 + \lambda \eta_1^2 .$$

The group is the first hypoabelian group if $\lambda = 0$; the second hypoabelian group if $\lambda = \lambda'$, where λ' is a particular mark such that

$$\xi_1 \eta_1 + \lambda' \xi_1^2 + \lambda' \eta_1^2$$

is not decomposable into linear factors in $GF\,[2^n]$.

The conditions for the invariance of F_λ under (34) are the abelian relations (35) and (36) for $\mu = 1$, together with

$$\sum_{j=1}^{m} \alpha_{ij}\gamma_{ij} + \lambda \alpha_{i1}^2 + \lambda \gamma_{i1}^2 = \begin{cases} 0, & (i = 2, \ldots, m) \\ \lambda, & (i = 1) \end{cases}, \tag{41}$$

$$\sum_{j=1}^{m} \beta_{ij}\delta_{ij} + \lambda \beta_{i1}^2 + \lambda \delta_{i1}^2 = \begin{cases} 0, & (i = 2, \ldots, m) \\ \lambda, & (i = 1) \end{cases}. \tag{42}$$

For $p = 2$, the inverse of a special abelian substitution is obtained by replacing $\alpha_{ij}, \beta_{ij}, \gamma_{ij}, \delta_{ij}$ by $\delta_{ji}, \beta_{ji}, \gamma_{ji}, \alpha_{ji}$ respectively. From (35), (36), (41), (42) may therefore be obtained an equivalent set of conditions. It follows readily that the transposed of the matrix of a hypoabelian substitution is the matrix of a hypoabelian substitution.

The group G_λ contains a subgroup J_λ of index 2 defined by the additional condition (A. J., p. 231):

$$\sum_{i,j}^{1,\ldots,m} \alpha_{ij}\delta_{ij} + \lambda^2 (\alpha_{11}^2 + \beta_{11}^2 + \gamma_{11}^2 + \delta_{11}^2) = m . \tag{43}$$

If $m > 1$, the group $J_{\lambda'}$ is simple; if $m > 2$, the group J_0 is simple.

22. THEOREM.—*The groups J_λ possess successive generality.*

We are to prove that, for any set of marks, not all zero, of the $GF[2^n]$ satisfying conditions (35), (36), (41), (42) for $i, k = 1, 2, \ldots, t$, $k \neq i$, where t is any given positive integer $< 2m$, there exists in J_λ a substitution S which replaces ξ_l and η_l by respectively

$$X_l \equiv \sum_{j=1}^{m} (\alpha_{lj}\xi_j + \gamma_{lj}\eta_j), \quad Y_l \equiv \sum_{j=1}^{m} (\beta_{lj}\xi_j + \delta_{lj}\eta_j),$$

for each $l = 1, 2, \ldots, \tau$, in case $t = 2\tau$; but also replaces $\xi_{\tau+1}$ by $X_{\tau+1}$ if $t = 2\tau + 1$.

The theorem has already been proved for $t = 1$. Indeed,[*] for any set of marks, not all zero, of the $GF[2^n]$ such that

$$\sum_{j=1}^{m} \alpha_{1j}\gamma_{1j} = 0,$$

there exists in J_0 a substitution replacing ξ_1 by X_1. Also (A. J., p. 233), for any set of marks of the $GF[2^n]$ satisfying

$$\sum_{j=1}^{m} \alpha_{1j}\gamma_{1j} + \lambda'\alpha_{11}^2 + \lambda'\gamma_{11}^2 = \lambda',$$

there exists in $J_{\lambda'}$ a substitution which replaces ξ_1 by X_1.

To prove the theorem for $t = 2$, let α_{1j}, γ_{1j}, β_{1j}, δ_{1j} be any set of marks of the $GF[2^n]$ such that

$$\sum_{=1}^{m} (\alpha_{1j}\delta_{1j} - \gamma_{1j}\beta_{1j}) = 1, \quad \sum_{j=1}^{m} \alpha_{1j}\gamma_{1i} + \lambda\alpha_{11}^2 + \lambda\gamma_{11}^2 = \lambda,$$

$$\sum_{j=1}^{m} \beta_{1j}\delta_{1j} + \lambda\beta_{11}^2 + \lambda\delta_{11}^2 = \lambda. \qquad (44)$$

By the case $t = 1$ just established, J_λ contains a substitution A and its inverse A^{-1}, both exhibited in §18, such that $\alpha'_{1j} \equiv \alpha_{1j}$, $\gamma'_{1j} \equiv \gamma_{1j}$. Also there exists a linear substitution S_1, with coefficients in the $GF[2^n]$ of determinant not zero, which replaces ξ_1 by X_1 and η_1 by Y_1. Hence, the product $A^{-1}S_1 \equiv R$ leaves ξ_1 fixed and replaces η_1 by the function ρ of §18, where, in particular, $r_1 = 1$. We proceed to prove that* (mod 2)

---

[*] Bull. Amer. Math. Soc., vol. IV (1898), p. 498.

$$\sum_{j=1}^{m} \rho_j r_j + \lambda \rho_1^2 = \lambda - \lambda r_1^2 = 0. \tag{45}$$

By a simple arrangement of the summation indices, we have

$$\begin{aligned}\sum_{j=1}^{m} \rho_j r_j = \sum_{i,\,k}^{1,\,\ldots\,,\,m} \beta_{1i}\delta_{1k} \sum_{j=1}^{m} (\alpha'_{jk}\delta'_{ji} + \beta'_{jk}\gamma'_{ji}) + \sum_{i=1}^{m} \beta_{1i}^2 \sum_{j} \delta'_{ji}\gamma'_{ji} + \sum_{i=1}^{m} \delta_{1i}^2 \sum_{j} \alpha'_{ji}\beta'_{ji} \\ + \sum_{i<k}^{1,\,\ldots\,,\,m} \beta_{1i}\beta_{1k} \sum_{j=1}^{m} (\delta'_{ji}\gamma'_{jk} + \delta'_{jk}\gamma'_{ji}) + \sum_{i<k}^{1,\,\ldots\,,\,m} \delta_{1i}\delta_{1k} \sum_{j=1}^{m} (\alpha'_{ji}\beta'_{jk} + \alpha'_{jk}\beta'_{ji}) \\ = \sum_{i=1}^{m} \beta_{1i}\delta_{1i} + \sum_{i=2}^{m} \beta_{1i}^2 (\lambda\delta_{1i}'^2 + \lambda\gamma_{1i}'^2) + \beta_{11}^2 (\lambda + \lambda\delta_{11}'^2 + \lambda\gamma_{11}'^2) \\ + \sum_{i=2}^{m} \delta_{1i}^2 (\lambda\alpha_{1i}'^2 + \lambda\beta_{1i}'^2) + \delta_{11}^2 (\lambda + \lambda\alpha_{11}'^2 + \lambda\beta_{11}'^2),\end{aligned}$$

since the coefficients of $\beta_{1i}\beta_{1k}$, $\delta_{1i}\delta_{1k}$ and $\beta_{1i}\delta_{1k}$ (the latter if $i \neq k$) vanish, while that of $\beta_{1i}\delta_{1k}$ ($i = k$) is unity, in view of the abelian conditions (35) and (36) when written for the inverse of (34) [see §21]. The other reductions were made by using the relations corresponding to (41) and (42) for the inverse. Adding the term

$$\lambda\rho_1^2 \equiv \lambda \sum_{i=1}^{m} (\beta_{1i}^2 \delta_{1i}'^2 + \delta_{1i}^2 \beta_{1i}'^2) \quad (\text{mod } 2)$$

and setting $\alpha'_{1j} = \alpha_{1j}$, $\gamma'_{1j} = \gamma_{1j}$, we obtain the sum

$$\sum_{i=1}^{m} \beta_{1i}\delta_{1i} + \lambda\beta_{11}^2 + \lambda\delta_{11}^2 + \lambda \sum_{i=1}^{m} (\beta_{1i}^2\gamma_{1i}^2 + \delta_{1i}^2\alpha_{1i}^2),$$

which $\equiv 0$ (mod 2) in view of the first and third relations (44). By the origin of R and S_1, the product $S_1 = AR$ replaces ξ_1 by X_1 and η_1 by Y_1.

Inversely, if R' be any substitution which replaces ξ_1 by ξ_1 and η_1 by ρ, the product AR' will replace ξ_1 and η_1 by X_1 and Y_1. Hence, if R' can be chosen to belong to J_λ, the required hypoabelian substitution S may be taken to be AR'. In view of relation (45), there exists in J_λ, for $\lambda = 0$, such a substitution R' (Bulletin, l. c., p. 498). For $\lambda = \lambda'$, there exists in J_λ such a substitution R' (A. J., p. 234).

---

*A shorter, but indirect, proof is sketched in §26. The third relation (44) would form the basis, its left member being identified with F^λ of §21.

By a similar method we may establish the general case of the theorem by one-stage induction [compare §5].

Since the relation (43), distinguishing the subgroup J_λ from the total hypoabelian group G_λ, involves the coefficients of all the rows of the matrix, it does not affect the cases of the theorem for which $t < 2m$. But for $t = 2m$, the theorem is evident from the definition of the group. Hence, the above proof shows also that *the groups G_λ possess successive generality.*

23. In the definition of $G_{\lambda'}$, the indices ξ_1, η_1 play a special rôle, and hence the coefficients α_{1j}, β_{1j}, γ_{1j}, δ_{1j}, α_{j1}, β_{j1}, γ_{j1}, δ_{j1}, enter in a special way into the relations (41), (42), and the analogous relations derived from the inverse substitutions.

By a change of notation, ξ_m and η_m may be given the special rôle, and hence also the coefficients of the last row and last column of the matrix. From this new standpoint the groups possess successive generality, the first case of the theorem being known (A. J., pp. 227–8).

24. For any one of the $N^{(\lambda)}_{m,n}$ sets of solutions (not all zero) in the $GF[2^n]$ of

$$\sum_{j=1}^{m} a_{1j}c_{1j} + \lambda a_{11}^2 + \lambda c_{11}^2 = \lambda, \tag{46}$$

these exists (§22) in J_λ a substitution T replacing ξ_1 by $\sum_{j=1}^{m} (a_{1j}\xi_j + c_{1j}\eta_j)$. If therefore S be any substitution of J_λ, the product ST will belong to J_λ and hence will replace ξ_1 by a function $\Sigma\, (a'_{1j}\xi_j + c'_{1j}\eta_j)$, whose coefficients satisfy (46). All such linear functions are therefore permuted transitively by J_λ. For $\lambda = 0$, ξ_i, $\eta_i\, (i = 1, \ldots, m)$ occur among these linear functions; a substitution of J_0 which leaves them all fixed is the identity. For $\lambda = \lambda'$, the functions

$$\xi_1 + \xi_2,\ \eta_1 + \xi_2,\ \xi_i,\ \eta_i \qquad (i = 2, \ldots, m)$$

occur among the above linear functions defined by (46). A substitution of J'_λ which leaves them fixed is evidently the identity. Similar remarks hold for the groups G_λ. We may therefore state the theorem:

If $m > 1$, the groups J_λ and G_λ may be represented as transitive substitution groups on $N^{(\lambda)}_{m,n}$ letters.

The number of sets of solutions of (46) is known (*A. J.*, p. 230, p. 235):

$$N^{(0)}_{m,n} = (2^{nm} - 1)(2^{n(m-1)} + 1), \quad N^{(\lambda')}_{m,n} = (2^{nm} + 1)\, 2^{n(m-1)}.$$

In the evaluation for $\lambda = 0$, the set of solutions $a_{1j} = c_{1j} = 0$ $(j = 1, \ldots, m)$ has been excluded. For $\lambda = 0$, (46) is homogeneous, so that we may group the linear functions into sets of $2^n - 1$ each, those of one set differing only by a constant factor. The resulting symbols

$$\{a_{11}\xi_1 + c_{11}\eta_1 + \ldots + a_{1m}\xi_m + c_{1m}\eta_m\},$$

are permuted transitively by J_0. A substitution S leaving every symbol fixed multiplies each index by a constant* ρ; if S belong to J_0, the abelian condition (35), for $\mu = 1$, gives $\rho^2 = 1$, whence $\rho \equiv 1$ modulo 2.

If $m > 1$, *the groups* J_0 *and* G_0 *may be represented as transitive substitution groups on* $(2^{nm} - 1)(2^{n(m-1)} + 1)/(2^n - 1)$ *letters.*

25. We next treat $J_{\lambda'}$ from the standpoint indicated in §23. For any set of solutions (not all zero) in the $GF[2^n]$ of

$$\sum_{j=1}^{m} a_{mj}c_{mj} + \lambda' a_{m1}^2 + \lambda' c_{m1}^2 = 0, \tag{47}$$

there exists (A. J., p. 227) in $J_{\lambda'}$ a substitution which replaces ξ_m by

$$\sum_{j=1}^{m} (a_{mj}\xi_j + c_{mj}\eta_j).$$

The number of such sets of solutions is (A. J., p. 230)

$$(2^{nm} + 1)(2^{n(m-1)} - 1).$$

Proceeding as in §24, we obtain the theorem†:

If $m > 1$, *the groups* $J_{\lambda'}$ *and* $G_{\lambda'}$ *may be represented as transitive substitution groups on* $(2^{nm} + 1)(2^{n(m-1)} - 1)/(2^n - 1)$ *letters.*

This number is less than the number $N_{m,n}^{(\lambda')}$ of §24.

26. To obtain a representation of J_0 upon a smaller number of letters than that given by the last theorem of §24, we employ the general method used for

---

[*] Consider in connection with the symbols $\{\xi_1\}$, $\{\eta_1\}$, $\{\xi_2\}$, etc., also the symbols $\{\xi_1 + \xi_2\}$, $\{\xi_1 + \eta_2\}$, etc. The various multipliers are thus seen to be equal.

[†] A substitution of $J_{\lambda'}$ is the identity if it leave fixed the symbols

$$\{\xi_i\},\ \{\eta_i\},\ \{\xi_1 + \lambda'^{\frac{1}{2}}\xi_i + \lambda'^{\frac{1}{2}}\eta_i\},\ \{\eta_1 + \lambda'^{\frac{1}{2}}\xi_i + \lambda'^{\frac{1}{2}}\eta_i\} \qquad (i = 2, \ldots, m),$$

since ξ_i and η_i are multiplied by the same constant [unity by (35)] and since a like result holds for ξ_1 and η_1.

the orthogonal groups (§8, seq). The functions $a_{11}\xi_1 + c_{11}\eta_1 + \dots + a_{1m}\xi_m + c_{1m}\eta_m$ in which

$$\sum_{j=1}^{m} (a_{1j}c_{1j} + \lambda a_{11}^2 + \lambda c_{11}^2 = c = \text{constant} \tag{48}$$

are permuted amongst themselves by the substitutions of G_λ. The simplest proof may be based upon §3, noting first that the left member of (48) has the form of the defining invariant F_λ of the group G_λ (§21) and secondly that the transposition of the matrix of a hypoabelian substitution leads to a hypoabelian substitution. A proof following the method of §8 results from the computation of (45) made in §22.

The case $c = 0$ has been treated in §§24–25. For different values of $c \neq 0$, relation (48) has evidently the same number of sets of solutions, since every mark of the $GF\ [2^n]$ is a square. For $\lambda = \lambda'$, we take $c = \lambda'$ and have the case treated in §24.

There remains the case $\lambda = 0$, $c \neq 0$, when we take $c = 1$. From the known number of solutions of (46), for $\lambda = 0$, we derive at once the result that the equation

$$\sum_{j=1}^{m} a_{1j}\, c_{1j} = 1 \tag{48'}$$

has in the $GF\,[2^n]$ the following number of sets of solutions:

$$(2^{nm} - 1)(2^{nm} - 2^{n(m-1)})/(2^n - 1) \equiv (2^{nm} - 1)\, 2^{n(m-1)}.$$

Among the functions $a_{11}\xi_1 + c_{11}\eta_1 + \dots$ defined by (48′) occur (if $m > 1$),

$$\xi_1 + \eta_1, \quad \xi_1 + \eta_1 + \xi_i, \quad \xi_1 + \eta_1 + \eta_i, \quad \xi_2 + \eta_2 + \xi_1, \\ (i = 2, \dots, m).$$

A substitution on the ξ_i, η_i, which leaves fixed all of these functions, will leave fixed every index and, therefore, be the identity. The isomorphism of G_λ with the substitution group is therefore holoedric. We may state the result:

If $m > 1$, *the groups* J_0 *and* G_0 *may be represented as transitive substitution groups on* $(2^{nm} - 1)\, 2^{n(m-1)}$ *letters.*

27. Comparing the number of letters required by the final theorem of §24 for the representation of J_0 and G_0 with the number of letters required by §26,

we find that the former is less than the latter if $n > 1$ but is greater if n 1. For $n = 1$, these numbers are $2^{2m-1} + 2^{m-1} - 1$ and $2^{2m-1} - 2^{m-1}$ respectively.* For this case ($n = 1$) our results for the representation of the first hypoabelian group as transitive substitution groups agree with the results of the lengthy investigation by M. Jordan upon the groups of Steiner.† As we are now in a position to pass directly from any hypoabelian substitution to the corresponding substitution of the isomorphic substitution group, the results of M. Jordan may be proven quite simply. This investigation and the generalization to arbitrary n will be deferred to a later paper.

THE UNIVERSITY OF CHICAGO, *February*, 1901.

---

* By §25, J_λ' for $n = 1$ may be represented transitively on $2^{2m-1} - 2^{m-1} - 1$ letters. Adjoining the symbol $\{ 0 \}$, we obtain an intransitive representation upon the same number of letters as employed for the group J_0.

† "Traité des substitutions," pp. 229–249. See particularly Nos. 318, 347. In the defining congruence No. 318, line 5, the right member should read 1 instead of 0.